(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2003198544 A

(43) Date of publication of application: 11.07.03

(51) Int. Cl H04L 9/32
G06F 15/00
G09C 1/00
H04L 9/08

(21) Application number: 2002301924

(22) Date of filing: 16.10.02

(30) Priority: 19.10.01 JP 2001321656

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

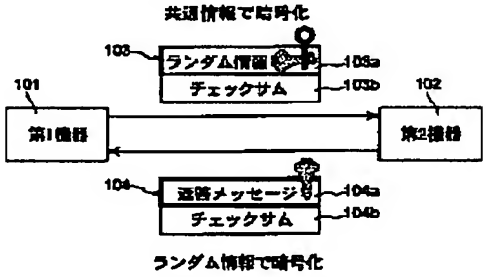
(72) Inventor: YAMAMOTO MASAYA
MIURA YASUSHI
NAKAHARA TORU

(54) EQUIPMENT AUTHENTICATION SYSTEM AND EQUIPMENT AUTHENTICATION METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To provide an equipment authentication system for certain equipment to securely specify the other equipment included in the same group as the present equipment when all the equipment are equal since it is estimated that processing such as copy or move of contents is permitted only within a certain fixed range when performing such processing among a plurality of equipments.

SOLUTION: Transmission data 103 to be transmitted from a first equipment 101 is composed of random information 103a and a checksum 103b enciphered by common information, and transmitted to a second equipment 102. The second equipment 102 receives the transmission data 103 and returns reply data 104 composed of an answer message 104a and a checksum 104b enciphered by the random information 103a to the first equipment 101.



(2)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－198544
（P2003－198544A）
(43)公開日　平成15年７月11日(2003.7.11)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
H04L 9/32		G06F 15/00	330A	5B085
G06F 15/00	330		330E	5J104
		G09C 1/00	640E	
G09C 1/00	640	H04L 9/00	675A	
H04L 9/08			601C	

審査請求　未請求　請求項の数33　ＯＬ　（全 22 頁）　最終頁に続く

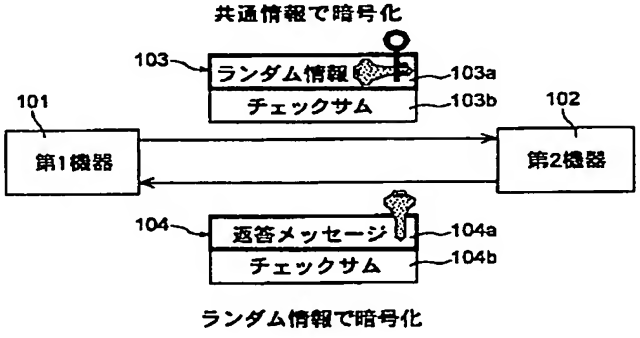
(21)出願番号　特願2002－301924(P2002－301924)
(22)出願日　平成14年10月16日(2002.10.16)
(31)優先権主張番号　特願2001－321656(P2001－321656)
(32)優先日　平成13年10月19日(2001.10.19)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　山本　雅哉
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　三浦　康史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100109210
弁理士　新居　広守

最終頁に続く

(54)【発明の名称】　機器認証システムおよび機器認証方法

(57)【要約】
【課題】　複数の機器間においてコンテンツのコピーや移動といった処理をする場合、それらの処理はある一定の範囲内においてのみ許可されることが想定される。全ての機器が対等の関係となる場合において、ある機器が自らと同一のグループに含まれる他の機器をセキュアに特定する機器認証システムを提供する。
【解決手段】　第１機器１０１より送信される送信データ１０３は、共通情報で暗号化されたランダム情報１０３ａ、及びチェックサム１０３ｂにより構成され、第２機器１０２へ送信される。前記第２機器１０２は、前記送信データ１０３を受信して、前記ランダム情報１０３ａで暗号化した返答メッセージ１０４ａ、及びチェックサム１０４ｂで構成される返信データ１０４を前記第１機器１０１へ返信する。



【特許請求の範囲】

【請求項１】　少なくとも第１及び第２機器から構成され、前記第１及び前記第２機器が同一のグループに属するか否かを判定する機器認証システムであって、
前記第１機器は、
共通情報を記憶する第１共通情報記憶手段と、
鍵情報を含む送信データを生成する送信データ生成手段と、
生成された送信データを前記共通情報で暗号化する第１暗号化手段と、
前記第１暗号化手段で得られた暗号化送信データを前記第２機器に送信する第１送信手段と、
前記第２機器から送られてきた暗号化返信データを前記鍵情報で復号化する第１復号化手段と、
復号化された前記返信データが一定の規則を有するか否か判定し、一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断する認証手段とを備え、
前記第２機器は、
共通情報を記憶する第２共通情報記憶手段と、
前記第１機器から送られてきた暗号化送信データを前記共通情報で復号化する第２復号化手段と、
復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、
前記送信データが一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、
生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第２暗号化手段と、
前記第２暗号化手段で得られた暗号化返信データを前記第１機器に送信する第２送信手段とを備えることを特徴とする機器認証システム。

【請求項２】　前記送信データ生成手段は、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲１記載の機器認証システム。

【請求項３】　前記第１機器は、さらに、前記送信データのチェックサムを生成するチェックサム生成手段を備え、
前記第１送信手段は、前記暗号化送信データとともに、前記チェックサムを前記第２機器に送信し、
前記判定手段は、復号化された前記送信データのチェックサムが前記第１機器から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲１記載の機器認証システム。

【請求項４】　前記第２機器は、前記判定手段による判定により復号化された前記送信データが一定の規則を有しない場合は、前記返信データを前記第１機器に返信しないことを特徴とする請求の範囲１記載の機器認証システム。

【請求項５】　前記第１暗号化手段は、前記送信データと前記チェックサムとを連結して暗号化し、
前記第１送信手段は、前記第１暗号化手段で得られた暗号化データを前記第２機器に送信し、
前記第２復号化手段は、前記第１機器から送られてきた暗号化データを前記共通情報で復号化することによって、送信データとチェックサムとに復号し、
前記判定手段は、復号化された前記送信データのチェックサムが復号化された前記チェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲１記載の機器認証システム。

【請求項６】　前記送信データ生成手段は、予め定められた固定情報を含む送信データを生成し、
前記判定手段は、復号化された前記送信データに含まれる固定情報が予め定められたデータパターンであるか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲１記載の機器認証システム。

【請求項７】　前記機器認証システムには、前記第２機器が複数含まれ、
前記第１送信手段は、複数の第２機器に対して前記送信データをブロードキャストすることを特徴とする請求の範囲１記載の機器認証システム。

【請求項８】　前記機器認証システムには、前記第２機器が複数含まれ、
前記第１送信手段は、複数の第２機器に対して前記送信データを送信し、
前記第１機器は、さらに、
前記認証手段による前記複数の第２機器に対する判断に基づいて、当該第１機器と同一グループに属する第２機器の一覧を示すグループリストを生成するグループリスト生成手段と、
生成されたグループリストに基づいて、第２機器と一定の通信を行うグループ通信手段とを備えることを特徴とする請求の範囲１記載の機器認証システム。

【請求項９】　前記第１機器は、さらに、前記グループリストに登録される第２機器の数が一定数を超えないように、前記送信データ生成手段、前記第１送信手段及び前記グループリスト生成手段の少なくとも１つを制御することを特徴とする請求の範囲８記載の機器認証システム。

【請求項１０】　前記送信データ生成手段は、前記送信データのサイズが一定長となるように、送信データにパディングデータを含ませ、
前記返信データ生成手段は、前記返信データのサイズが一定長となるように、返信データにパディングデータを含ませることを特徴とする請求の範囲１記載の機器認証

システム。

【請求項１１】　前記送信データ生成手段は、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、

前記第２機器は、さらに、復号化された前記送信データに含まれる検索情報が示す物を当該第２機器が保持するか否か判定する検索情報判定手段を備え、

前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成することを特徴とする請求の範囲１記載の機器認証システム。

【請求項１２】　前記送信データ生成手段は、デジタルコンテンツを特定するコンテンツＩＤを前記検索情報として前記送信データに含ませ、

前記返信データ生成手段は、前記送信データに含まれているコンテンツＩＤが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第２機器が保持する場合に、当該ライセンスを特定するライセンスＩＤを前記返信データに含ませることを特徴とする請求の範囲１１記載の機器認証システム。

【請求項１３】　前記第１機器は、さらに、

前記第２機器から送られてきた返信データに含まれるライセンスＩＤの一覧を示すリストを生成するリスト生成手段と、

生成されたリストに基づいて、前記第２機器とライセンスの授受のための通信を行う通信手段とを備えることを特徴とする請求の範囲１２記載の機器認証システム。

【請求項１４】　前記第１共通情報記憶手段及び前記第２共通情報記憶手段は、それぞれ、複数の異なる共通情報を記憶し、

前記第１暗号化手段は、前記第１共通情報記憶手段に記憶された複数の共通情報の中から選択した１つの共通情報を用いて前記送信データを暗号化し、

前記第２復号化手段は、前記第２共通情報記憶手段に記憶された複数の共通情報の中から選択した１つの共通情報を用いて前記送信データを復号化することを特徴とする請求の範囲１記載の機器認証システム。

【請求項１５】　前記送信データ生成手段は、デジタルコンテンツ及びその利用形態を特定する情報を検索情報として前記送信データに含ませて前記送信データを生成し、

前記第２機器は、さらに、復号化された前記送信データに含まれる検索情報が示すデジタルコンテンツの前記利用形態による利用を可能にする権利情報であるライセンスを当該第２機器が保持するか否か判定する検索情報判定手段を備え、

前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成し、

前記第１暗号化手段は、前記第１共通情報記憶手段に記憶された複数の共通情報の中から前記利用形態に対応した１つの共通情報を選択し、選択した共通情報を用いて前記送信データを暗号化し、

前記第２復号化手段は、前記第２共通情報記憶手段に記憶された複数の共通情報の中から前記利用形態に対応した１つの共通情報を選択し、選択した共通情報を用いて前記送信データを復号化することを特徴とする請求の範囲１４記載の機器認証システム。

【請求項１６】　前記第１機器は、さらに、前記第１共通情報記憶手段に記憶されている共通情報の追加及び削除を行う第１共通情報編集手段を備え、

前記第２機器は、さらに、前記第２共通情報記憶手段に記憶されている共通情報の追加及び削除を行う第２共通情報編集手段を備えることを特徴とする請求の範囲１５記載の機器認証システム。

【請求項１７】　少なくとも第１及び第２機器から構成され、前記第１及び前記第２機器が同一のグループに属するか否かを判定するシステムにおける機器認証方法であって、

前記第１機器及び前記第２機器は、それぞれ、共通情報を記憶する第１共通情報記憶手段及び第２共通情報記憶手段を備え、

前記機器認証方法は、

前記第１機器において、

鍵情報を含む送信データを生成する送信データ生成ステップと、

生成された送信データを前記共通情報で暗号化する第１暗号化ステップと、

前記第１暗号化ステップで得られた暗号化送信データを前記第２機器に送信する第１送信ステップと、

前記第２機器から送られてきた暗号化返信データを前記鍵情報で復号化する第１復号化ステップと、

復号化された前記返信データが一定の規則を有するか否か判定し、一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断する認証ステップとを含み、

前記第２機器において、

前記第１機器から送られてきた暗号化送信データを前記共通情報で復号化する第２復号化ステップと、

復号化された前記送信データが一定の規則を有するか否かを判定する判定ステップと、

前記送信データが一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成ステップと、

生成された返信データを前記復号化ステップで復号された送信データに含まれていた鍵情報で暗号化する第２暗号化ステップと、

前記第２暗号化ステップで得られた暗号化返信データを前記第１機器に送信する第２送信ステップとを含むこと

を特徴とする機器認証方法。

【請求項１８】　前記送信データ生成ステップでは、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲１７記載の機器認証方法。

【請求項１９】　前記機器認証方法は、さらに、

前記第１機器において、前記送信データのチェックサムを生成するチェックサム生成ステップを含み、

前記第１送信ステップでは、前記暗号化送信データとともに、前記チェックサムを前記第２機器に送信し、

前記判定ステップでは、復号化された前記送信データのチェックサムが前記第１機器から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲１７記載の機器認証方法。

【請求項２０】　前記第１暗号化ステップでは、前記送信データと前記チェックサムとを連結して暗号化し、

前記第１送信ステップでは、前記第１暗号化ステップで得られた暗号化データを前記第２機器に送信し、

前記第２復号化ステップでは、前記第１機器から送られてきた暗号化データを前記共通情報で復号化することによって、送信データとチェックサムとに復号し、

前記判定ステップは、復号化された前記送信データのチェックサムが復号化された前記チェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲１７記載の機器認証方法。

【請求項２１】　前記システムには、前記第２機器が複数含まれ、

前記第１送信ステップは、複数の第２機器に対して前記送信データを送信し、

前記第１機器は、さらに、

前記認証ステップによる前記複数の第２機器に対する判断に基づいて、当該第１機器と同一グループに属する第２機器の一覧を示すグループリストを生成するグループリスト生成ステップと、

生成されたグループリストに基づいて、第２機器と一定の通信を行うグループ通信ステップとを含むことを特徴とする請求の範囲１７記載の機器認証方法。

【請求項２２】　前記送信データ生成ステップでは、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、

前記機器認証方法は、さらに、前記第２機器において、復号化された前記送信データに含まれる検索情報が示す物を当該第２機器が保持するか否か判定する検索情報判定ステップを含み、

前記返信データ生成ステップでは、前記検索情報判定ステップによる判定結果を前記返信データに含ませて前記返信データを生成することを特徴とする請求の範囲１７記載の機器認証方法。

【請求項２３】　前記送信データ生成ステップでは、デジタルコンテンツを特定するコンテンツＩＤを前記検索情報として前記送信データに含ませ、

前記返信データ生成ステップでは、前記送信データに含まれているコンテンツＩＤが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第２機器が保持する場合に、当該ライセンスを特定するライセンスＩＤを前記返信データに含ませることを特徴とする請求の範囲２２記載の機器認証方法。

【請求項２４】　前記第１共通情報記憶手段及び前記第２共通情報記憶手段は、それぞれ、複数の異なる共通情報を記憶し、

前記第１暗号化ステップでは、前記第１共通情報記憶手段に記憶された複数の共通情報の中から選択した１つの共通情報を用いて前記送信データを暗号化し、

前記第２復号化ステップでは、前記第２共通情報記憶手段に記憶された複数の共通情報の中から選択した１つの共通情報を用いて前記送信データを復号化することを特徴とする請求の範囲１７記載の機器認証方法。

【請求項２５】　相手装置と相互に認証し合うことによって、相手装置と自装置とが同一グループに属するか否かを判定する通信装置であって、

相手装置を認証するための認証部と、

相手装置から認証してもらうための被認証部とを備え、

前記認証部は、

共通情報を記憶する共通情報記憶手段と、

鍵情報を含む送信データを生成する送信データ生成手段と、

生成された送信データを前記共通情報で暗号化する第１暗号化手段と、

前記第１暗号化手段で得られた暗号化送信データを前記相手装置に送信する第１送信手段と、

前記相手装置から送られてきた暗号化返信データを前記鍵情報で復号化する第１復号化手段と、

復号化された前記返信データが一定の規則を有するか否か判定し、一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断する認証手段とを有し、

前記被認証部は、

前記相手装置から送られてきた暗号化送信データを前記共通情報で復号化する第２復号化手段と、

復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、

前記送信データが一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、

生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第２暗号化手段と、

前記第２暗号化手段で得られた暗号化返信データを前記

相手装置に送信する第２送信手段とを有することを特徴とする通信装置。

【請求項２６】　前記送信データ生成手段は、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲２５記載の通信装置。

【請求項２７】　前記相手装置は、さらに、前記送信データのチェックサムを生成するチェックサム生成手段を備え、

前記第１送信手段は、前記暗号化送信データとともに、前記チェックサムを前記相手装置に送信し、

前記判定手段は、復号化された前記送信データのチェックサムが前記相手装置から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲２５記載の通信装置。

【請求項２８】　相手装置と相互に認証し合うことによって、相手装置と自装置とが同一グループに属するか否かを判定する通信装置のためのプログラムであって、

相手装置を認証するための認証ステップと、

相手装置から認証してもらうための被認証ステップとを含み、

前記認証ステップは、

鍵情報を含む送信データを生成する送信データ生成ステップと、

生成された送信データを予め記憶している共通情報で暗号化する第１暗号化ステップと、

前記第１暗号化ステップで得られた暗号化送信データを前記相手装置に送信する第１送信ステップと、

前記相手装置から送られてきた暗号化返信データを前記鍵情報で復号化する第１復号化ステップと、

復号化された前記返信データが一定の規則を有するか否か判定し、一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断する認証ステップとを含み、

前記被認証ステップは、

前記相手装置から送られてきた暗号化送信データを前記共通情報で復号化する第２復号化ステップと、

復号化された前記送信データが一定の規則を有するか否かを判定する判定ステップと、

前記送信データが一定の規則を有する場合に、前記相手装置は自装置と同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成ステップと、

生成された返信データを前記復号化ステップで復号された送信データに含まれていた鍵情報で暗号化する第２暗号化ステップと、

前記第２暗号化ステップで得られた暗号化返信データを前記相手装置に送信する第２送信ステップとを含むことを特徴とするプログラム。

【請求項２９】　前記送信データ生成ステップは、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする請求の範囲２８記載のプログラム。

【請求項３０】　前記プログラムは、さらに、前記送信データのチェックサムを生成するチェックサム生成ステップを含み、

前記第１送信ステップは、前記暗号化送信データとともに、前記チェックサムを前記相手装置に送信し、

前記判定ステップは、復号化された前記送信データのチェックサムが前記相手装置から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする請求の範囲２８記載のプログラム。

【請求項３１】　少なくとも第１及び第２機器から構成され、前記第１及び前記第２機器が同一のグループに属するか否かを判定する機器認証システムに用いられる認証データが記録されたコンピュータ読み取り可能な記録媒体であって、

前記認証データには、

鍵情報を含む送信データが共通情報で暗号化された暗号化送信データと、

前記送信データのチェックサムとが含まれ、

前記認証データは、前記第１機器から前記第２機器に送信されるデータであり、

前記鍵情報は、前記第１機器が前記第２機器と同一のグループに属すると前記第２機器が判断した場合に、前記第２機器が前記第１機器に返信する返信データの暗号化に用いられ、

前記共通情報は、同一のグループに属する機器が予め保持する情報であることを特徴とする記録媒体。

【請求項３２】　前記鍵情報は、前記第１機器で生成された乱数であることを特徴とする請求の範囲３１記載の記録媒体。

【請求項３３】　前記送信データには、デジタルコンテンツを特定するコンテンツＩＤが含まれ、

前記返信データには、前記送信データに含まれているコンテンツＩＤが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを特定するライセンスＩＤが含まれることを特徴とする請求の範囲３１記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、同一ネットワークにおいて各機器が他の機器の認証を行う場合に必要となる機器認証システムに関するものであり、特に、複数の端末機器間における機器認証システムに関するものである。

【０００２】

【従来の技術】近年、音楽や映像、ゲーム等デジタルコ

ンテンツはインターネットやデジタル放送及び、パッケージメディアによる流通により容易に取得が可能となってきている。そうしたデジタルコンテンツ及びその権利を複数の端末間においてコピーや移動を行う際には、無制限な範囲での移動は許されず、ある一定範囲内でのコピーや移動のみが許されるのが一般的である。

【０００３】一般的には同一ユーザが所有する複数の端末間においてのみコピーや移動が許されると考えられている。このような一定範囲内でのコピーや移動を実現するためには、当該端末群によってコピーや移動が相互に可能なグループを形成する必要がある。

【０００４】従来、このようなグループの判定はサーバ（グループ判定端末）が行うことが想定されている。以下、サーバにおけるグループ判定について簡単に説明する。

【０００５】従来のグループ判定システムはグループの判定を行うサーバとネットワークとにより通信可能に接続される被管理端末群からなる。サーバはグループごとに該当する端末のグループリストを保持している。グループリストとは例えばグループ識別子と端末識別子とを関連付ける情報である。

【０００６】以上の構成のグループ判定システムでは、以下のようにグループの判定が行われる。まず、被管理端末は自らが属するグループの端末リストを取得する場合、サーバに端末リスト要求データを送信する。前記端末リスト要求データには、例えば自らの端末識別子、グループ識別子といったものが含まれる。サーバは端末リスト要求データに含まれる情報に従って該当するグループリストを前記被管理端末に送信する。以上の処理を経て被管理端末は自らの属するグループ情報を取得することによりグループの判定を実現している。

【０００７】例えば、従来のメンバー識別方法では、ホスト端末が全メンバー及びホスト端末固有のネットワークアドレスをデータとしたパケットを同報送信し、メンバー端末は、受信パケットを解析し自分の名前の入ったパケットからの情報を取り出して識別し、各メンバー名と各メンバー端末固有のネットワークアドレスをデータとするパケットをホスト端末へ送信し、ホスト端末は、受信パケットを解析し、同一グループに属するメンバーの名前があった場合には、そのパケットに含まれる情報を取得し、メンバー名と端末アドレスとを対応させ、対応データをセーブしてグループの識別を行っている（例えば、特許文献１参照。）。

【０００８】

【特許文献１】特開平１０－２３０２８号公報

【０００９】

【発明が解決しようとする課題】まず、従来のグループ判定方法が抱えている問題点について説明すると、従来のグループ判定方法においては、サーバ端末（グループ判定端末）と被管理端末とには親子関係が生じ、サーバ端末と被管理端末とで異なる機能を持つ必要がある。

【００１０】次に、従来の判定方法を一般的なユーザが使用する家電製品等に適応することを考える。従来の判定方法を適用するにはユーザは自らの保持する家電製品の親子関係を把握し、かつ購入時にどのように親子関係を設定するかも想定しながら購入する必要がある。なぜならグループ判定においてサーバ端末は必須であり、またサーバ端末と被管理端末とは機能や価格等が異なることが想定されるためである。

【００１１】本来、家電製品のように随時端末が追加されていき、様々な利用の仕方が想定される端末は、端末間の関係が対等であるべきと考えられる。つまり、従来は全ての端末が対等の関係となる場合にグループを構成するための方法は知られていない。

【００１２】そこで、前記課題に鑑み、本発明に係る機器認証システムにおいては、各端末機器も対等の関係になる場合において同一グループに属する機器の特定を可能とする。

【００１３】また、本発明に係る機器認証システムは、端末機器が認証処理、コンテンツ送受信処理等の端末に負荷の大きい処理を行う前に、安全に同一グループに属する端末のグループリストを取得することを目的とする。そして、本発明に係る機器認証システムは、前記グループリストを利用することにより、送信データの送信先となる機器を決定して、コンテンツの取得が不可能な端末に対しては通信を行わずに、通信経路の効率的な利用等を可能とすることを目的とする。

【００１４】さらに、本発明は、将来のコンテンツの有料ネットワーク配信の普及に対応した機器認証システムを提供することをも目的とする。

【００１５】

【課題を解決するための手段】前記目的を達成するために、本発明に係る機器認証システムでは、少なくとも第１及び第２機器から構成され、前記第１及び前記第２機器が同一のグループに属するか否かを判定する機器認証システムであって、前記第１機器は、共通情報を記憶する第１共通情報記憶手段と、鍵情報を含む送信データを生成する送信データ生成手段と、生成された送信データを前記共通情報で暗号化する第１暗号化手段と、前記第１暗号化手段で得られた暗号化送信データを前記第２機器に送信する第１送信手段と、前記第２機器から送られてきた暗号化返信データを前記鍵情報で復号化する第１復号化手段と、復号化された前記返信データが一定の規則を有するか否か判定し、一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断する認証手段とを備え、前記第２機器は、共通情報を記憶する第２共通情報記憶手段と、前記第１機器から送られてきた暗号化送信データを前記共通情報で復号化する第２復号化手段と、復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、前記送信

データが一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第２暗号化手段と、前記第２暗号化手段で得られた暗号化返信データを前記第１機器に送信する第２送信手段とを備えることを特徴とする。

【００１６】また、前記目的を達成するために、本発明は、前記送信データ生成手段は、乱数を生成し、生成した乱数を前記鍵情報として含む送信データを生成することを特徴とする。さらに、本発明は、前記第１機器は、さらに、前記送信データのチェックサムを生成するチェックサム生成手段を備え、前記第１送信手段は、前記暗号化送信データとともに、前記チェックサムを前記第２機器に送信し、前記判定手段は、復号化された前記送信データのチェックサムが前記第１機器から送信されてきたチェックサムと一致するか否かを判定することによって、前記一定の規則を有するか否かを判定することを特徴とする機器認証システムとなる。

【００１７】さらに、前記目的を達成するために、本発明に係る機器認証システムでは、前記機器認証システムには、前記第２機器が複数含まれ、前記第１送信手段は、複数の第２機器に対して前記送信データをブロードキャストする。

【００１８】そして、前記目的を達成するために、本発明に係る機器認証システムは、前記送信データ生成手段は、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、前記第２機器は、さらに、復号化された前記送信データに含まれる検索情報が示す物を当該第２機器が保持するか否か判定する検索情報判定手段を備え、前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成することを特徴とする。

【００１９】前記目的を達成するために、本発明に係る機器認証システムは、前記送信データ生成手段は、デジタルコンテンツを特定するコンテンツＩＤを前記検索情報として前記送信データに含ませ、前記返信データ生成手段は、前記送信データに含まれているコンテンツＩＤが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第２機器が保持する場合に、当該ライセンスを特定するライセンスＩＤを前記返信データに含ませることを特徴とする。

【００２０】尚、本発明は、上述のような機器認証システムとして実現できるのみではなく、この機器認証システムが備える手段をステップとする機器認証方法、及び当該手段を装置上で実現する通信装置としても実現することができる。

【００２１】また、前記機器認証方法をコンピュータ等で実現させるプログラムとして実現したり、当該プログラムをＣＤ－ＲＯＭ等の記録媒体や通信ネットワーク等の伝送媒体を介して流通させることができるのは言うまでもない。

【００２２】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態について説明し、本発明の理解に供する。尚、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定するものではない。以下、本発明に係る実施の形態について図面を用いて説明する。

【００２３】ここで詳細の説明に先立ち、本発明におけるグループの定義を行う。互いにコンテンツ又はコンテンツに対する権利をコピーや移動といった処理が相互に可能な端末が存在する場合に、それらの端末群は論理的にグルーピングが可能である。そしてグルーピングした端末群の属する単位を認可範囲(Authorized Domain)とし、以下、簡単のためグループと呼ぶ。

【００２４】（実施の形態１）図１は、本発明の実施の形態１に係る機器認証システムを説明する概略図である。図１において、第１機器１０１と第２機器１０２とは有線又は無線の伝送路を介してデータ通信可能に接続される。ここで、第１機器１０１は他の機器が自らと同一グループに属するか判定する機器に相当し、第２機器１０２は、自らのグループに属するか否かを尋ねてきた機器に対して、応答する機器に相当する。また、本実施の形態１においては、端末機器は第１機器１０１と第２機器１０２とで説明を行うが、ブロードキャストの到達範囲内における全ての端末機器に対して同様の方法により機器認証を行うことができる。

【００２５】第１機器１０１は、例えば、ユーザの利用する機器であり、ＰＣ、携帯電話、セットトップボックス等である。この第１機器１０１は、グループ化を行いグループリストを作成する機器であり、グループ化を行うために送信データ１０３を作成して、この送信データ１０３を暗号化して第２機器１０２へ送信する。

【００２６】第２機器１０２は、前記第１機器１０１と同様に、例えばＰＣ、携帯電話、セットトップボックス等の端末機であり、ブロードキャスト到達範囲内にあり、第１機器１０１より送信される送信データ１０３を受信して返信データ１０４を暗号化して第１機器１０１へ返送する。

【００２７】送信データ１０３は、ランダム情報１０３ａとチェックサム１０３ｂとを備えており、このランダム情報１０３ａは、第１機器１０１で生成されるランダムなバイト列であるパスワード等の共通情報により暗号化されている。また、チェックサム１０３ｂは、送信前にランダム情報１０３ａ等のデータを分割し、それぞれのブロック内のデータを数値とみなして合計した情報であり、本実施の形態１においては、暗号化はされずに送

信される。尚、このチェックサム１０３ｂを共通情報等により暗号化して送信することも可能である。

【００２８】返信データ１０４は、第１機器１０１より投げかけられた情報に返答するためのデータであり、返答メッセージ１０４ａとチェックサム１０４ｂとを含む。返答メッセージ１０４ａには、例えば同一グループであることが記載され、受信したランダム情報１０３ａを用いて暗号化される。また、チェックサム１０４ｂは、前記チェックサム１０３ｂと同様に、送信前に返答メッセージ１０４ａ等のデータを分割し、それぞれのブロック内のデータを数値とみなして合計した情報であり、本実施の形態１においては、暗号化はされずに返送される。

【００２９】図２を用いて第１機器１０１が他の機器に対して自らと同一グループに属するか否かを判定する場合の流れを説明する。尚、実施の形態１では同一グループに属するか否かは共通情報Ａを保持しているか否かに起因している。即ち、本発明の方法でグループ判定処理を行う場合、同一グループに属する機器は共通情報Ａを保持しておくことを前提としている。

【００３０】図２は、本実施の形態１に係る複数の機器とグループとの関係を示す図である。この機器認証システムは、第１機器１０１と、第２機器１０２と、第６機器２０１と、第７機器２０２とが存在し、本実施の形態１において、第１機器１０１は、自らと同じグループである他の機器をフィルタリングする機器に該当し、ブロードキャストにより他の機器に対して自らと同一グループに属するか否かを判定する。図２において、第１機器１０１と、第２機器１０２とは同一グループであるドメイン１(Authorized Domain１)に属し、第７機器２０２は別のグループとなるドメイン２(Authorized Domain２)に属するものとする。

【００３１】第１機器１０１は、ＰＣ等の端末機であり、通信可能なブロードキャスト到達範囲である第２機器１０２及び第７機器２０２に共通情報Ａで暗号化した送信データをブロードキャストする。ここで通信可能な範囲には、例えば家庭内のホームネットワーク等が含まれる。

【００３２】第２機器１０２は、共通情報Ａを保持しており、この共通情報Ａにより暗号化された送信データを復号化することができ、通信エラーを考えなければ正しい返信データを第１機器１０１へ返信することができる。また、第１機器１０１は、この返信データを受信し、所定の処理を行うことにより、第２機器１０２が同一グループに属すると判断する。

【００３３】第７機器２０２は、保持している共通情報Ｃが共通情報Ａと異なるため、共通情報Ａにより暗号化された送信データの受信後、所定の処理を行うと第７機器２０２に備えられているチェックサム判定部においてチェックサム不一致となり返信データを返さない。また、偶然、第７機器２０２のチェックサム判定においてチェックサムが一致したとしても、第１機器１０１のチェックサム判定によりチェックサム不一致となり、同一グループの機器リストとして第７機器２０２はフィルタリングされない。尚、ブロードキャスト到達範囲外にある第６機器２０１は、送信データが到達しないため同一グループと判定されることはない。

【００３４】以上の判定方法により、第１機器１０１は、共通情報Ａを送信することなく同一グループに属する機器のグループリストを作成することができる。このグループリストに含まれる機器は、少なくとも同一の共通情報Ａを保持することが保証され、即ち同一グループに属することが保証される。

【００３５】以下、第１機器１０１及び第２機器１０２について順番に、それぞれの詳細な構成について説明する。図３は、本実施の形態１に係る第１機器１０１の詳細な構成を示すブロック図である。第１機器１０１は、ブロードキャストを行い同一グループに属する端末機器のグループリスト構成を行う端末であり、ランダムなバイト列を生成するランダム情報生成部３０１と、暗号／復号部３０２と、パスワード等の共通情報を記憶している共通情報記憶部３０３と、チェックサム生成部３０４と、機器間通信部３０５と、チェックサム判定部３０６を備えている。尚、前記チェックサムとは送信前のデータを分割し、それぞれのブロック内のデータを数値とみなして合計を取ったものである。

【００３６】まず第１機器１０１が第２機器１０２へ送信データＴ－Ｄａｔａ１を送信する場合のデータの流れについて説明する。ランダム情報生成部３０１は、ランダムなバイト列を生成し、このバイト列をセッション鍵情報、パディングデータ等のランダム情報Ｒ１として用いると共に、このランダム情報Ｒ１をタイムアウト時間まで保持する。このタイムアウト時間とは、ランダム情報Ｒ１を生成してから他の機器からの返信を待つ最後の時間まで値を示し、機器においてユーザ或いは機器メーカーが設定する。また、ランダム情報生成部３０１は、ランダム情報Ｒ１をチェックサム生成部３０４及び暗号／復号部３０２へ送信する。

【００３７】暗号／復号部３０２は、共通情報Ａを用いてランダム情報Ｒ１の暗号化を行い、この暗号化された暗号化情報Ｅ１を機器間通信部３０５へ送信する。共通情報記憶部３０３は、共通情報Ａを記憶するハードディスク等を有しており、この共通情報Ａは、通常ユーザ自らが入力するのではなくサーバ側が管理しており、入会時や購入時においてサーバ側より共通情報記憶部３０３へ入力される情報である。

【００３８】チェックサム生成部３０４は、受信した前記ランダム情報Ｒ１のチェックサム対象部のデータのブロック内のデータの数値の合計をＣＳ１として生成し、このＣＳ１を機器間通信部３０５へ送信する。そして、

機器間通信部３０５は、受信したチェックサムＣＳ１と暗号化情報Ｅ１とにより送信データＴ－Ｄａｔａ１のパケットを構築して、これを送信データＴ－Ｄａｔａ１として第２機器１０２側へ送信する。

【００３９】一方、第１機器１０１が第２機器１０２から返送された返信データＡ－Ｄａｔａ２を受信する場合のデータの流れについて説明する。まず、機器間通信部３０５は、他の機器である第２機器１０２とデータの送受信を行い、受信した返信データＡ－Ｄａｔａ２のうち暗号化情報Ｅ２を復号化するため暗号／復号部３０２へ送信すると共に、返信データＡ－Ｄａｔａ２に付与されているＣＳ３をチェックサム判定部３０６へ送信する。

【００４０】暗号／復号部３０２は、暗号化情報Ｅ２の復号化をランダム情報Ｒ１を用いることにより行い、復号化された復号済み応答データＤＡ２をチェックサム生成部３０４へ送信する。チェックサム生成部３０４は、受信した前記復号済み応答データＤＡ２のチェックサム対象部のデータのブロック内のデータの数値の合計をＣＳ４として生成し、このＣＳ４をチェックサム判定部３０６へ送信する。

【００４１】チェックサム判定部３０６は、同一グループに属する機器を記憶する記憶部であるグループリストを備えており、前記ＣＳ３と前記ＣＳ４との比較を行い、判定の結果、一致する場合には第２機器１０２を同一グループに属する機器としてグループリストへ追加する。また、判定の結果チェックサムが一致しない場合には、第２機器１０２を同一グループに属さない機器と判断してグループリストへの追加を行わない。尚、前記復号済み応答データＤＡ２は暗号／復号部３０２が送信するとしたが、チェックサム判定部３０６が取得要求を送信するとしてもよい。

【００４２】図４は、本実施の形態１に係る第２機器１０２の詳細な構成を示すブロック図である。第２機器１０２は、前記第１機器１０１と同様な暗号／復号部４０２と、共通情報記憶部４０３と、チェックサム生成部４０４と、機器間通信部４０５と、チェックサム判定部４０６との構成に加えて、さらに、同一グループに属する等の情報を含む応答データＡＤを生成する応答データ生成部４０７を備えている。尚、第１装置１０１に備えられるランダム情報生成部３０１は備えられていない。

【００４３】第２機器１０２が第１機器１０１から受信する送信データＴ－Ｄａｔａ１の流れについて説明すると、機器間通信部４０５は、送信データＴ－Ｄａｔａ１を受信し、この送信データＴ－Ｄａｔａ１のうち暗号化情報Ｅ１を暗号／復号部４０２へ送信すると共に、ＣＳ１をチェックサム判定部４０６へ送信する。

【００４４】暗号／復号部４０２は、共通情報記憶部４０３に記憶されている共通情報Ａにより前記暗号化情報Ｅ１の復号化を行い、復号化された復号化済みデータＤＲ１をチェックサム生成部４０４へ送信する。

【００４５】チェックサム生成部４０４は、前記復号化済みデータＤＲ１のチェックサム対象部のデータのブロック内のデータの数値の合計をＣＳ２として生成し、このＣＳ２をチェックサム判定部４０６へ送る。チェックサム判定部４０６においては、前記ＣＳ１と前記ＣＳ２との比較を行い、判定の結果一致していれば、同一グループの属する機器からの送信データＴ－Ｄａｔａ１として応答データ生成部４０７へ応答データＡＤの作成を指示する。

【００４６】応答データ生成部４０７は、前記指示により、同一グループに属する等のデータを含んだ応答データＡＤの生成を行い、この応答データＡＤを暗号／復号部４０２とチェックサム生成部４０４とへ送信する。暗号／復号部４０２は、応答データＡＤを暗号化情報Ｅ１に含まれるランダム情報Ｒ１で暗号化して暗号化データＥ２として機器間通信部４０５へ送る。また、チェックサム生成部４０４は、応答データＡＤのチェックサム対象部のデータのブロック内のデータの数値の合計をＣＳ３として生成して機器間通信部４０５へ送る。尚、前記暗号化においてはランダム情報Ｒ１を用いて暗号化するのではなく、共通情報Ａを用いて暗号化することもできる。

【００４７】機器間通信部４０５は、前記暗号化データＥ２と前記ＣＳ３とを含んだパケットデータである返信データＡ－Ｄａｔａ２を生成して第１機器１０１側へ返送し、一連の機器認証システムにおけるデータ処理を終了する。

【００４８】図５は、本実施の形態１に係る送信データＴ－Ｄａｔａ１のデータ構成を示す図である。尚、この図５は、本実施の形態１の説明のために例示するものである。

【００４９】送信データＴ－Ｄａｔａ１は、第１機器１０１より他の機器へ送信され、他の機器が第１機器１０１と同一グループに属するか否かの返答要求メッセージであり、メッセージヘッダ５０１、クライアントＩＤ５０２、ランダム情報５０３、パディングデータ５０４、チェックサム５０５より構成されている。

【００５０】メッセージヘッダ５０１は、同一グループに属するか否かのメッセージ等を含み、送信データＴ－Ｄａｔａ１の先頭領域に位置しており、暗号化されずに送信されるデータである。クライアントＩＤ５０２は、メッセージ送信元である第１機器１０１のクライアントＩＤが保持されている。

【００５１】ランダム情報５０３は、ランダムなバイト列で構成され、返信データを暗号化する際に用いられるセッション鍵等の情報を含む。このセッション鍵の情報は、タイムアウト時間まで第１機器１０１側において保持され、返信データの暗号化部を復号化する際に用いられる情報である。

【００５２】パディングデータ５０４は、予備的なデー

タであり、例えば、暗号アルゴリズムがＡＥＳであり、送信データＴ－Ｄａｔａ１のデータ長が暗号化単位の８バイトの倍数となっていない際に送信データＴ－Ｄａｔａ１が８バイトの倍数となるように付与されるデータである。そして、共通情報により暗号化され、暗号強度を増すためにパディングデータ５０４で暗号化対象データ部ＥＤを長くしてもよい。尚、パディングデータ５０４の代わりに２バイト程度のリザーブフィールドを設けることも考えられる。

【００５３】チェックサム５０５は、クライアントＩＤ５０２とランダム情報５０３とパディングデータ５０４とから成るチェックサム対象部ＣＴのデータのブロック内のデータの数値の合計を保持している。また、ＣＲＣ３２のようなチェックサム・アルゴリズムの代わりにハッシュ関数を用いてもよく、例えばＳＨＡ－１やＭＤ５としてもよい。

【００５４】暗号化対象データＥＤは、クライアントＩＤ５０２、ランダム情報５０３、及びパディングデータ５０４により構成され、少なくともランダム情報５０３を含むものとする。また、暗号化対象データＥＤには第１機器１０１をネットワーク上で一意に識別する機器識別情報を含んでもよい。ここで機器識別情報は、具体的には自らのＩＰアドレス、機器の識別子であるクライアントＩＤ５０２等となる。尚、返信データを返送する場合等にＩＰアドレスが必要であれば、送信データＴ－Ｄａｔａ１にＩＰアドレスを含めることも可能である。

【００５５】図６を用いて返信データＡ－Ｄａｔａ２の内容について説明する。図６は、本実施の形態１に係る返信データＡ－Ｄａｔａ２のデータ構成を示す図である。尚、この図６は、本実施の形態１の説明のために例示するものであり、本発明はこの構成に限定されるものではない。

【００５６】返信データＡ－Ｄａｔａ２は、第１機器１０１より送信される返答要求メッセージである送信データＴ－Ｄａｔａ１に対する返信である。この返信データＡ－Ｄａｔａ２は、メッセージヘッダ６０１、クライアントＩＤ６０２、共通情報６０３、パディングデータ６０４、及びチェックサム６０５より構成される。

【００５７】メッセージヘッダ６０１は、同一グループに属するか否かのメッセージ等であり、クライアントＩＤ６０２は返信データＡ－Ｄａｔａ２の送信元となる第２機器１０２のクライアントＩＤである。共通情報６０３は、第１機器１０１と第２機器１０２とが共通して有しているパスワード等の共通情報であり、本実施の形態１においては共通情報Ａである。

【００５８】パディングデータ６０４は、予備的なデータであり、暗号強度を増すためにパディングデータ６０４で応答データＡＤを長くすることも可能である。チェックサム６０５は、クライアントＩＤ６０２と共通情報６０３とパディングデータ６０４とから成るチェックサム対象部ＣＴのデータのブロック内のデータの数値の合計である。

【００５９】応答データＡＤは、クライアントＩＤ６０２と共通情報６０３とパディングデータ６０４とより成り、第２機器１０２が共通情報Ａを保持していることを確認するために共通情報６０３を含んでいる。この応答データＡＤは、前記ランダム情報５０３に含まれるセッション鍵等を用いて暗号化されてから返信される。

【００６０】また、応答データＡＤは、少なくとも第２機器１０２をネットワーク上で一意に識別する機器識別情報を含む。ここで機器識別情報は、自らのＩＰアドレス、機器の識別子であるクライアントＩＤ６０２等を想定する。尚、応答データＡＤは少なくとも機器識別情報を含むとしたが、機器間において通信を行う場合に付与される通信プロトコルに応じたメッセージヘッダに機器識別情報相当（例えば自らのＩＰアドレス）の情報が含まれる場合はこの限りではない。

【００６１】本発明の機器認証システムを用いる準備としての共通情報の機器への設定の仕方について以下に例を示す。図７は、本実施の形態１におけるユーザインターフェイスの画面を示す図である。グループの設定範囲は、一般に同一ユーザが所有する複数の機器群を想定している。グループの設定を行うユーザは共通情報を何らかの方法で入手し、同一グループに属する機器に図７（ａ）に示すようなＵＩで入力処理を行う。尚、機器に共通情報を設定するユーザを限定するためパスワード等を設けてもよい。ユーザの共通情報の入手方法については、図７（ｂ）に示すように、例えば、ある機器の共通情報である「zeppetstore」を表示させ、それを同一グループに設定する他の機器に入力する。また、共通情報は機器メーカー、販売店等から葉書やｅメール等により入手してもよいし、ユーザが考えて同一グループに設定する他の機器に設定してもよい。

【００６２】また、共通情報はユーザには提示せず、機器メーカー、販売店等がユーザの要求、或いはメーカー、販売店のポリシーにより出荷時、販売時に設定してもよい。そして、ＩＣカードに共通情報を記憶し、各機器が挿入したＩＣカードの情報を読み込むことにより共通情報を設定するとしてもよい。尚、ＩＣカードの入手方法は共通情報の入手で上述したようにあらゆる方法を想定する。また、ＩＣカードの代わりに記憶媒体、或いはＳＤカード等のデータをセキュアに管理できる記憶媒体を用いてもよい。

【００６３】尚、通常は、ユーザが共通情報等を自ら入力するのではなく、サーバ側が管理して、サーバ側よりグループ入会時、ＰＣ購入時等において各端末機器へ伝送路を介して自動的に入力される。このため、ユーザが共通情報を知ることにより、同一グループに属する対象となる端末機器が故意に広がってしまう可能性を防止する。

【００６４】次に、第１機器１０１が作成するグループリストの情報項目についての内容の一例を説明する。図８は、本実施の形態１における第１機器１０１が作成するグループリストの情報項目を示す図である。図８（ａ）においてグループを識別するグループＩＤ（８０１ａ）の項目があり、グループＩＤ（８０１ａ）に対してグループに属する機器の識別情報が記述される。機器の識別情報としてはデバイスＩＤ（８０２ａ、８０３ａ）等を記述する。また、グループＩＤ（８０１ａ）に対応してグループの範囲内で許される可能な処理について記述してもよい。この可能な処理としては、図８（ａ）においては「コピー」であり、他には再生、移動等も考えられる。

【００６５】図８（ｂ）においても同様であり、グループを識別するグループＩＤ（８１１ｂ）の項目があり、グループＩＤ（８１１ｂ）に対してグループに属する機器の識別情報としてデバイスＩＤ（８１２ｂ、８１３ｂ）等を記述する。また、図８（ｂ）において、範囲内で許される可能な処理は「移動」である。

【００６６】また、機器ごとに複数のグループに属していてもよく、その場合、機器は複数のグループに対応する複数の共通情報を保持し、処理により図８（ａ）又は（ｂ）のように複数のグループＩＤに対するグループリストを保持することも可能とする。

【００６７】グループリストの生成が完了すると、グループリストに含まれる機器と通信を行い、同一グループ内で許可されている処理等を行う。以降の認証処理、コンテンツ取得処理等は一般的な方法でセキュアに行う。尚、グループリストはコンテンツのコピーや移動の処理の度に生成し、処理終了後、即時削除することにすれば、処理の度に常に最新のグループ情報を取得することが可能となる。

【００６８】本実施の形態１においては、ユーザメリットとなるグループ設定、及びグループ判定方法について説明するが、コンテンツホルダーの立場からはグループの定義範囲をあまり広げたくない場合も想定される。そのような場合はグループリストに記述できる機器識別情報の最大値を設定し、他の端末からの返信データによりグループリストを作る際に、最大値に達したらグループリストの生成処理を強制的に終了するようにしてもよい。以上の処理を行い、常に機器は正常に動作し、かつネットワーク構成が変わらないことを前提とすると、ユーザは最大値＋αくらいの機器しか同一グループに設定できなくなる。少なくともグループ内の機器を無限に増やすことを防ぐことが可能となる。

【００６９】また、同一グループの設定については上述したが、共通情報の新規入力や削除の処理により同一グループ内に属する機器を柔軟かつ容易に設定可能である。

【００７０】次に、以上のように構成された本実施の形態１に係る機器認証システムの動作について説明する。図９は、本実施の形態１に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。尚、本実施の形態１においては、第１機器１０１が、第２機器１０２と同一グループに属するか否かを判定する場合の説明を行うが、同様の機器認証システムを用いることにより、ブロードキャスト等において複数の端末機器間においても同一グループ判定を行うことが可能である。また、機器認証システムの動作の説明においては、図３及び図４の符号を参照するものとする。

【００７１】最初に、第１機器１０１を構成するランダム情報生成部３０１は、ランダム情報Ｒ１を生成し、同じく第１機器１０１を構成する暗号／復号部３０２、及びチェックサム生成部３０４に送信する（ステップ９０１）。尚、本実施の形態１においては、ランダム情報生成部３０１は、タイムアウト時間まではランダム情報Ｒ１を保持しておかなければならない。また、タイムアウト時間前であってもユーザによる終了指示によりランダム情報Ｒ１をランダム情報生成部３０１から削除してもよい。また、ランダム情報Ｒ１は何バイトかのランダムなバイト列であり、バイト数については暗号／復号処理に用いる暗号アルゴリズム等に依存する。

【００７２】続いて、暗号／復号部３０２は、ランダム情報生成部３０１よりランダム情報Ｒ１を受信すると共通情報記憶部３０３に共通情報取得要求を送信し、共通情報記憶部３０３より共通情報Ａを受信する。次に、暗号／復号部３０２は、少なくともランダム情報Ｒ１を含む暗号化対象データＥＤを共通情報Ａを鍵として暗号化を行い、暗号化情報Ｅ１を生成し、機器間通信部３０５に送信する（ステップ９０２）。ここで暗号のアルゴリズムとしては一般的に暗号強度が使用に耐えうるものを採用し、例えばＤＥＳ、ＴｒｉｐｌｅＤＥＳ、ＡＥＳ等を想定する。尚、以下では暗号／復号部３０２及び図４における暗号／復号部４０２は１つの同じ暗号アルゴリズムを保持することとして記述するが、複数の暗号アルゴリズムを保持してもよい。但し、複数暗号アルゴリズムを保持する場合は暗号アルゴリズム識別子が必要となるし、第１機器１０１及び第２機器１０２が前記暗号アルゴリズム識別子に対応する同じ暗号アルゴリズムを保持しておかなければならない。

【００７３】次に、チェックサム生成部３０４は、少なくともランダム情報Ｒ１を含む前記暗号化対象データＥＤに対するＣＳ１を生成し、機器間通信部３０５に送信する（ステップ９０３）。

【００７４】機器間通信部３０５は、暗号化情報Ｅ１と前記ＣＳ１との両者を受信すると少なくとも前記暗号化情報Ｅ１と前記ＣＳ１とを含み、通信プロトコルに応じたメッセージヘッダ等を付した送信データＴ－Ｄａｔａ１を他の機器に対して送信する（ステップ９０４）。

【００７５】次に、第２機器１０２に備えられる機器間

通信部４０５は、第１機器１０１より前記送信データＴ－Ｄａｔａ１を受信し、送信データＴ－Ｄａｔａ１より前記暗号化情報Ｅ１と前記ＣＳ１とを抽出する（ステップ９０５）。

【００７６】次に、機器間通信部４０５は、暗号化情報Ｅ１を同じく第２機器１０２を構成する暗号／復号部４０２へ、ＣＳ１を同じく第２機器１０２を構成するチェックサム判定部４０６へ送信する。

【００７７】暗号／復号部４０２は、暗号化情報Ｅ１を受信すると、共通情報記憶部４０３に共通情報取得要求を送信し、共通情報記憶部４０３より共通情報Ａを受信する。暗号／復号部４０２は暗号化情報Ｅ１を共通情報Ａを鍵として復号化を行い、復号された暗号化情報（以下、復号済み暗号化対象データと呼ぶ）ＤＲ１を取得し、チェックサム生成部４０４に送信する（ステップ９０６）。また、暗号／復号部４０２は応答データ生成部４０７から応答データＡＤが送信されてくるまで、取得した復号済み暗号化対象データＤＲ１を保持する。

【００７８】続いて、チェックサム生成部４０４は、受信した復号済み暗号化対象データＤＲ１に対するＣＳ２を生成し、チェックサム判定部４０６へ送信する（ステップ９０７）。チェックサム判定部４０６は受信したＣＳ１とＣＳ２との比較処理を行う（ステップ９０８）。

【００７９】そして、チェックサム判定部４０６は、比較処理の結果、ＣＳ１＝ＣＳ２となった場合はチェックサム一致の制御コードを、ＣＳ１≠ＣＳ２の場合はチェックサム不一致の制御コードを応答データ生成部４０７に送信する。

【００８０】応答データ生成部４０７は、チェックサム不一致の制御コードを受信した場合、応答データは生成しない（ステップ９０９）。尚、応答データＡＤを意味のないバイト列であるパディングデータ等で埋めたり、エラーコードを記述するとしてもよいが、本実施の形態１ではチェックサム不一致の場合、応答データＡＤを生成しないこととして説明を進める。また、チェックサム不一致の場合、チェックサム判定部４０６が応答データ生成部４０７に制御コードを送信しないとしてもよい。

【００８１】応答データ生成部４０７は、制御コードを受信し、制御コードに応じた応答データＡＤを生成し、暗号／復号部４０２及びチェックサム生成部４０４に送信する（ステップ９１０）。

【００８２】尚、正しい応答データＡＤを第１機器１０１に返信した機器は少なくとも同一グループに属しているという判断を行うため、チェックサムの不一致が通信エラーに起因するものであっても同様の判断を行ってよい。

【００８３】続いて、暗号／復号部４０２は、受信した応答データＡＤを保持している復号済み暗号化対象データＤＲ１からランダム情報Ｒ１を抽出し、セッション鍵等のランダム情報Ｒ１を鍵として暗号化を行い、暗号化情報Ｅ２を生成し、機器間通信部４０５に送信する（ステップ９１１）。また、チェックサム生成部４０４は受信した応答データＡＤに対するＣＳ３を生成し、機器間通信部４０５に送信する（ステップ９１２）。機器間通信部４０５は暗号化情報Ｅ２とＣＳ３との両者を受信すると、少なくとも暗号化情報Ｅ２とＣＳ３とを含み、通信プロトコルに応じたメッセージヘッダ等を付した返信データＡ－Ｄａｔａ２を第１機器１０１に対して送信する（ステップ９１３）。

【００８４】次に、第１機器１０１に備えられる機器間通信部３０５は、第２機器１０２より返信データＡ－Ｄａｔａ２を受信し、暗号化情報Ｅ２とＣＳ３とを抽出する（ステップ９１４）。次に、機器間通信部３０５は、暗号化情報Ｅ２を暗号／復号部３０２へ、ＣＳ３をチェックサム判定部３０６へ送信する。

【００８５】暗号／復号部３０２は、機器間通信部３０５より暗号化情報Ｅ２を受信するとランダム情報生成部３０１にランダム情報取得要求を送信し、ランダム情報生成部３０１よりランダム情報Ｒ１を受信する。暗号／復号部３０２は、受信した暗号化情報Ｅ２を同じく保持していたランダム情報Ｒ１を鍵として復号化を行い、復号された暗号化情報（以下、復号済み応答データと呼ぶ）ＤＡ２を取得し、チェックサム生成部３０４及びチェックサム判定部３０６に送信する（ステップ９１５）。尚、チェックサム判定部３０６に送る際に復号済み応答データＤＡ２より機器識別情報を抽出して送信してもよい。

【００８６】続いて、チェックサム生成部３０４は、受信した復号済み応答データＤＡ２に対するＣＳ４を生成し、チェックサム判定部３０６へ送信する（ステップ９１６）。チェックサム判定部３０６は受信したＣＳ３とＣＳ４との比較処理を行う（ステップ９１７）。

【００８７】まず、比較処理の結果、ＣＳ３＝ＣＳ４となった場合は応答データＡＤを送信してきた第２機器１０２が同一グループに属すると判断し、第２機器１０２が同一グループに属する機器としてリストに追加する（ステップ９１９）。一方、ＣＳ３≠ＣＳ４の場合は同一グループに属しないと判断し処理を終了する（ステップ９１８）。また、第２機器１０２のチェックサム不一致と同様の理由で、チェックサムの不一致が通信エラーに起因するものであっても同様の判断を行う。以上、第１機器１０１と第２機器１０２との間での機器認証システムの詳細を説明した。

【００８８】尚、本実施の形態１においては、送信データＴ－Ｄａｔａ１及び返信データＡ－Ｄａｔａ２の暗号化対象部はそれぞれ暗号化対象データＥＤ及び応答データＡＤであり、チェックサム５０５及びチェックサム６０５は含まれていないが、チェックサム５０５及びチェックサム６０５も含めて暗号化することができる。

【００８９】すなわち、第１機器１０１の送信データＴ

－Ｄａｔａ１の作成において、チェックサム対象部ＣＴのチェックサム５０５を算出した後にチェックサム対象部ＣＴとチェックサム５０５とを共に共通情報Ａにより暗号化する。そして、暗号化されたチェックサム対象部ＣＴとチェックサム５０５とを含む送信データＴ－Ｄａｔａ１を第２機器１０２へ送信する。一方、第２機器１０２においては、受信した送信データＴ－Ｄａｔａ１を共通情報Ａを用いて復号化して、一連の処理を行った後にランダム情報５０３により暗号化情報Ｅ２とチェックサムＣＳ３とを暗号化して返信データＡ－Ｄａｔａ２として返信することも可能である。

【００９０】以上のように、本実施の形態１に係る機器認証システムにおいては、第１機器１０１より送信される送信データＴ－Ｄａｔａ１は、共通情報Ａを用いて暗号化されたランダム情報５０３等を含む暗号化対象データＥＤとチェックサム５０５とを含む。そして、第２機器１０２は、暗号化対象データＥＤを共通情報Ａで復号化して、チェックサム５０５の一致の判定を行うことにより第１機器１０１が同一グループに属するか否かの判定を行い、同一グループに属する場合には、ランダム情報５０３で暗号化された暗号化情報Ｅ２、及びチェックサム６０５を含む返信データＡ－Ｄａｔａ２を第１機器１０１へ返送する。次に、第１機器１０１は、返信データＡ－Ｄａｔａ２を受信し、保持していたランダム情報５０３により応答データＡＤの復号化を行い、チェックサム６０５の一致判定により第２機器１０２が同一グループに属するか否かの判定を行い、チェックサムが一致する場合には、第２機器１０２をグループリストに追加する。

【００９１】このため、本実施の形態１における機器認証システムにおいて、第１機器１０１は、共通情報Ａを他の機器へ送信することなく同一グループに属する機器のグループリストを自ら作成することができ、認証処理、コンテンツ送受信処理等の第１機器１０１に負荷の大きい処理を行う前に、安全に同一グループに属する機器のグループリストを取得することができる。

【００９２】また、本実施の形態１における機器認証システムにおいては、同一グループに属する機器のグループリスト作成を第１機器１０１自らがサーバに依らず任意に行うことができ、ブロードキャスト等を行い、複数の機器間における同一グループ化を行う場合に有効となる。

【００９３】また、本実施の形態１に係る機器認証システムでは、各端末機器が共通情報Ａを有する対等の関係である場合において、各機器は、前記グループリストに従いデータの通信先を決定することにより、コンテンツの取得が不可能な機器に対して通信を行わない。このため、通信網の効率的な利用及びトラフィックの削減等を可能とする。

【００９４】さらに、本実施の形態１においては、乱数であるランダム情報Ｒ１を用いて返信データＡ－Ｄａｔａ２の暗号化及び復号化を行うことにより、より安全に第１機器１０１及び第２機器１０２間でのデータ送受信を行うことができ、以前の通信内容を入手して、同じ内容を送信することによって「なりすまし」等を行う攻撃であるリプレイ攻撃等をより効果的に回避することができる。

【００９５】尚、ここまで本実施の形態１では機器間で送受信されるデータはメッセージヘッダ５０１と暗号化された暗号化対象データＥＤと前記暗号化対象データＥＤに対するチェックサムとし、受信側である第２機器１０２でチェックサムの比較判定を行うとして説明した。ここで暗号化対象データＥＤに予め決められた固定情報を含め、受信側で固定情報が含まれるか否かにより同一の共通情報Ａを保持するか否かの判定を行うとしてもよい。即ち、機器間で送受信されるデータとしてはメッセージヘッダ５０１と固定情報を含む暗号化対象データＥＤを暗号化したものとしてよい。ここに固定情報を含むとは、例えば、暗号化対象データＥＤの先頭に「Ｈｅｌｌｏ」の文字列を挿入するということである。

【００９６】また、本実施の形態１では第２機器１０２において共通情報Ａを用いて同一グループに属するか否かの判定を行っているが、第２機器１０２において判定を行わず第１機器１０１においてのみ同一グループに属するか否かの判定を行うとしてもよい。例えば、第２機器１０２において受信した暗号化情報Ｅ１を共通情報Ａにより復号しランダム情報Ｒ１を取得する。ここでチェックサム判定を行わず（同じ共通情報Ａを保持しているかの判定を行わず）、応答データＡＤを前記ランダム情報Ｒ１を鍵として暗号化を行い第１機器１０１に返送する。第１機器１０１において復号化処理を行い、取得したデータが応答データＡＤとして正しいか否かの判定を行い、同一グループに属するか否かの判定を行うことも可能である。

【００９７】（実施の形態２）次に、本実施の形態２に係る機器認証システムについて説明する。尚、本実施の形態２においては、説明を容易にするために、前記実施の形態１と異なる点を中心に説明する。また、本実施の形態２は、デジタル著作物（コンテンツ）と、その利用を可能とする権利情報（ライセンス）とを分離した形態で管理すると共に、ネットワークを介してサーバから端末機器に配信するコンテンツ配信システムに関するものである。本実施の形態２では、同一グループ内の他の端末機器に格納されているライセンスを検索する処理への適用例を示す。

【００９８】図１０は、本実施の形態２に係る第３機器１００１の詳細な構成を示すブロック図である。この第３機器１００１は、本実施の形態２においては、前記第１機器１０１の構成に加えて、コンテンツ利用部１００１ａ、入力部１００５、及び検索情報付与部１００７を

備えている。

【００９９】コンテンツ利用部１００１ａは、サーバからブロードバンド等のネットワークを介して映画、音楽等のコンテンツ及びライセンスをダウンロードする際に利用され、映画等のコンテンツを記憶するコンテンツ記憶部１００２と、端末機器であるＰＣのユーザ等より発行を依頼されサーバ側において発行されたライセンスを記憶するライセンス記憶部１００３とを備え、さらに、コンテンツ記憶部１００２に記憶されたコンテンツをライセンスにより許可された利用条件に従って管理するための出力制御部１００４を備えている。尚、このコンテンツ利用部１００１ａの構成は説明のための例示であり、本実施の形態２の構成に限定されるものではない。

【０１００】コンテンツ記憶部１００２は、端末機器のユーザ側より購入処理を行い、サーバよりブロードバンド等を介してダウンロードされるコンテンツを格納する。このコンテンツは、通常サーバにおいてコンテンツ鍵を用いて暗号化された後に第３機器１００１側に送信される。

【０１０１】ライセンス記憶部１００３には、端末機器のユーザ等がサーバに発行依頼して取得するライセンスを保存する。このライセンスは、端末機器に対するコンテンツの利用許可を行うデータであり、また、当該ライセンスが関連付いているコンテンツのコンテンツＩＤ、コンテンツの利用形態を定めるアクションＩＤ、暗号化されたコンテンツの暗号化を解くコンテンツ鍵等を含み、さらに、コンテンツの機器上での利用条件を示す利用条件データが格納されている。この利用条件データには、有効期限（例えば、２００２年６月１日から２００２年８月３１日）、回数制限（例えば、１回再生が可能）、最大連続再生時間（例えば、１回の再生で最大１０時間再生が可能）等の情報が含まれる。尚、サーバで管理する利用条件としては、ライセンスに含まれる利用条件、サーバで管理把握できる情報（例えば、ユーザの利用履歴、ユーザの所持している機器リスト等）となる。

【０１０２】出力制御部１００４は、内蔵又はケーブルを介してテレビ、スピーカー、プリンタ等の再生機器と接続されており、第３機器１００１のユーザは、これら再生機器によってライセンスの利用許可範囲内においてコンテンツの利用を行う。また、出力制御部１００４と記録機器とを接続して、ＤＶＤやＳＤ等の蓄積メディアに対してコンテンツを記録することも可能となる。

【０１０３】入力部１００５は、第３機器１００１とネットワークを介して接続され、第３機器１００１に備えられるコンテンツ利用部１００１ａに対して、例えば、コンテンツ、ライセンス、ユーザ情報等の入力を行う。尚、この入力部１００５は、データベースを有するサーバ側で管理される。

【０１０４】端末管理部１００１ｂは、前記実施の形態１の第１機器１０１の構成に加えて、検索情報付与部１００７を備えている。まず、第３機器１００１が他の機器へ送信データＴ－Ｄａｔａ３を送信する場合のデータの流れを説明すると、ランダム情報生成部３０１及び検索情報付与部１００７は、ランダム情報Ｒ２及び検索情報Ｃを生成する。この検索情報Ｃは、検索対象のライセンスにて利用可能なコンテンツのＩＤ及びアクションのＩＤの情報を含む。尚、検索情報Ｃには、他の情報を含めることができる。そして、暗号／復号部３０２は、共通情報Ａにより検索情報Ｃとランダム情報Ｒ２と含む暗号化情報Ｅ３を生成し、この暗号化情報Ｅ３を機器間通信部３０５へ送信する。チェックサム生成部３０４においては、ランダム情報Ｒ２と検索情報ＣとによりＣＳ５を生成し、機器間通信部３０５は、暗号化情報Ｅ３とＣＳ５とを含む送信データＴ－Ｄａｔａ３を第４機器１１０１へ送信する。

【０１０５】一方、第３機器１００１が他の機器より返信データＡ－Ｄａｔａ４を受信する場合のデータの流れを説明すると、機器間通信部３０５は、第４機器１１０１より受信した返信データＡ－Ｄａｔａ４のうち暗号化されたデータＥ４を復号化するために暗号／復号部３０２へ送信すると共に、ＣＳ７をチェックサム判定部３０６に送信する。暗号／復号部３０２は、保持していたランダム情報Ｒ２を用いてデータＥ４の暗号化を解き、復号済み応答データＤＡ４をチェックサム生成部３０４に送信し、ここで生成されたＣＳ８をチェックサム判定部３０６へ送信する。チェックサム判定部３０６では、ＣＳ７とＣＳ８との比較を行い、判定の結果ＣＳ７とＣＳ８とが一致する場合には、第３機器１００１が作成するライセンスリストに第４機器１１０１が有している検索情報Ｃに当てはまるライセンスの情報を追加する。

【０１０６】図１１は、本実施の形態２に係る第４機器１１０１の詳細な構成を示すブロック図である。第４機器１１０１は、上述した第３機器１００１と同様に、コンテンツ利用部１１０１ａ、入力部１１０５、及び端末管理部１１０１ｂを備えている。また、コンテンツ利用部１１０１ａは、前記コンテンツ利用部１００１ａと同様の構成となる。

【０１０７】端末管理部１１０１ｂは、実施の形態１の第２機器１０２の構成に加えて、検索情報判別部１１０６を有している。端末管理部１１０１ｂが送信データＴ－Ｄａｔａ３を受信してから返信するまでの一連のデータの流れを説明すると、機器間通信部４０５は、送信データＴ－Ｄａｔａ３を受信し暗号化情報Ｅ３を暗号／復号部４０２へ送り、ＣＳ５をチェックサム判定部４０６へ送信する。暗号／復号部４０２では、共通情報Ａを用いて前記暗号化情報Ｅ３の復号化を行い、復号済み暗号化対象データＤＲ２をチェックサム生成部４０４に送信し、ここで生成されたＣＳ６をチェックサム判定部４０６に送信する。チェックサム判定部４０６では、ＣＳ５

とＣＳ６との比較を行う。比較の結果、チェックサムが一致しなかった場合には、送信データＴ－Ｄａｔａ３を無視する一方、チェックサムが一致する場合には、検索情報判別部１１０６は、コンテンツ利用部１１０１ａを検索して検索情報Cに当てはまるコンテンツに対応するライセンスの検索を行う。応答データ生成部４０７は、検索情報Ｃを満たすライセンスを発見できない場合には、応答データＡＤを作成しないが、検索情報Ｃを満たすライセンスを発見した場合には、ライセンス情報Ｃ２と応答データＡＤとを含む暗号化情報Ｅ４を作成し、機器間通信部４０５は、この暗号化情報Ｅ４とライセンス情報Ｃ２及び応答データＡＤから生成したＣＳ７とを含む返信データＡ－Ｄａｔａ４を第３機器１００１へ返信する。

【０１０８】図１２は、本実施の形態２に係る送信データＴ－Ｄａｔａ３のデータ構成を示す図である。尚、図１２は、本実施の形態２の説明のための例示である。

【０１０９】送信データＴ－Ｄａｔａ３は、他の機器が第３機器１００１と同一グループに属すると共に、検索情報に当てはまるライセンスの検索を行うように要求するメッセージであり、前記実施の形態１で説明した送信データＴ－Ｄａｔａ１の構成に加えて、コンテンツＩＤ１２０１及びアクションＩＤ１２０２のデータを含む。

【０１１０】コンテンツＩＤ１２０１は、要求するコンテンツのＩＤを示す。コンテンツには、少なくともコンテンツを一意に特定するための識別子がつけられており、通常、この識別子がコンテンツＩＤ１２０１となる。このコンテンツＩＤ１２０１は、検索対象のライセンスに対応するコンテンツのＩＤである。

【０１１１】アクションＩＤ１２０２は、前記コンテンツＩＤ１２０１に示されるコンテンツに対する利用形態を特定する識別子であり、また、検索対象のライセンスにて利用可能なアクションのＩＤとなる。このアクションとしては、例えば、視聴、再生、コピー、移動、プリント等である。

【０１１２】尚、これらコンテンツＩＤ１２０１及びアクションＩＤ１２０２は、共通情報Ａにより暗号化されてから送信される暗号化対象データＥＤに含まれ、また、本発明においても前記実施の形態１と同様に暗号化対象データＥＤのみでなく、チェックサム５０５も共に共通情報Ａにより暗号化して送信することも可能である。

【０１１３】図１３は、本実施の形態２に係る返信データＡ－Ｄａｔａ４のデータ構成を示す図である。この返信データＡ－Ｄａｔａ４は、第３機器１００１より送信される送信データＴ－Ｄａｔａ３に対する返信であり、実施の形態１の返信データＡ－Ｄａｔａ２の構成に加えて、ライセンスＩＤ１３０１及び利用条件データ１３０２が含まれている。

【０１１４】ライセンスＩＤ１３０１は、権利情報であるライセンスそのものではなく、検索情報Ｃのコンテンツに利用できるライセンスの識別番号であり、本実施の形態２においては、検索対象の端末である第４機器１１０１で検索されたライセンスを識別するための番号となる。

【０１１５】利用条件データ１３０２は、ライセンスにより許可されるコンテンツの利用条件を示すデータであり、通常ライセンスに含まれている。本実施の形態２においては、第３機器１００１等で判定される条件でコンテンツの操作内容であるアクション（例えば、視聴）を開始して良いか否かを判定するＣ条件（例えば、１０回）等のデータが含まれている。

【０１１６】尚、ライセンスＩＤ１３０１及び利用条件データ１３０２は、ランダム情報Ｒ２により暗号化される応答データＡＤに含まれている。

【０１１７】図１４は、本実施の形態２に係る第３機器１００１が検索情報Ｃを用いて第４機器１１０１及び第５機器１４０１にライセンス検索を行う際の通信手順を示すシーケンス図である。尚、本図においては、第５機器１４０１は共通情報Ａを有していないものとする。

【０１１８】まず、第３機器１００１は、同一グループ内の他の端末機器に格納されるライセンスを検索し、検索情報Ｃに含まれるコンテンツのライセンスを保持している機器のライセンスリストを作成することを目的とする。このために、共通情報Ａで暗号化した検索情報Ｃを含む送信データを第４機器１１０１及び第５機器１４０１に送信する（ステップ１４０２）。尚、この送信は、本実施の形態２においてはブロードキャストにより行われている。

【０１１９】次に、第４機器１１０１及び第５機器１４０１は、送信データを受信すると、共通情報Ａを用いて送信データのうち暗号化されたデータの復号化を行い、チェックサムの判定を行う（ステップ１４０３）。送信データを受信した第５機器１４０１は、共通情報Ａを有していないため暗号化された送信データの復号化が正しく行われず、チェックサムの不一致となり返信データは返信されない（ステップ１４０４）。

【０１２０】一方、第４機器１１０１は、共通情報Ａ及び検索情報Ｃを満たすか否かの判定を行い（ステップ１４０５）、満たしている場合には返信データにライセンス情報を付与して返信し（ステップ１４０７）、満たしていない場合には返信しない（ステップ１４０６）。そして、第３機器１００１は、図１４に示すように検索情報Ｃを満たすライセンスリスト１４０８を作成し、このライセンスリスト１４０８に従いデータの通信先を決定する。

【０１２１】図１５は、本実施の形態２に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。尚、図９を用いて実施の形態１に係る機器認証システムのグループ判定の処理手順を説明したが、実

施の形態１と同様の処理手順については、図９と同一のステップ番号を付すものとする。以下、図１５に従って、第３機器１００１が他の機器に対して自らと同一グループに属し、かつ検索情報Ｃを満たす他の機器のライセンスリスト１４０８を作成する場合の詳細な流れを説明する。

【０１２２】最初に、第３機器１００１に備えられるランダム情報生成部３０１は、ランダム情報Ｒ２を生成し（ステップ９０１）、また、検索情報付与部１００７は、検索対象のコンテンツＩＤ１２０１及びアクションＩＤ１２０２を有する検索情報Ｃを生成する（ステップ１５０１）。そして、ランダム情報Ｒ２及び検索情報Ｃを暗号／復号部３０２及びチェックサム生成部３０４に送信する。

【０１２３】続いて、暗号／復号部３０２は、ランダム情報生成部３０１よりランダム情報Ｒ２を受信すると共通情報記憶部３０３に共通情報取得要求を送信し、共通情報記憶部３０３より共通情報Ａを受信し、少なくともランダム情報Ｒ２及び検索情報Ｃを含む暗号化対象データＥＤを共通情報Ａを鍵として暗号化を行い、暗号化情報Ｅ３を生成し、機器間通信部３０５に送信する（ステップ９０２）。

【０１２４】次に、チェックサム生成部３０４は、少なくともランダム情報Ｒ２及び検索情報Ｃを含む暗号化対象データＥＤに対するＣＳ５を生成し、機器間通信部３０５に送信する（ステップ９０３）。

【０１２５】機器間通信部３０５は、暗号化情報Ｅ３とＣＳ５との両者を受信すると少なくとも前記暗号化情報Ｅ３と前記ＣＳ５とを含み、通信プロトコルに応じたメッセージヘッダ等を付した送信データＴ－Ｄａｔａ３を他の機器に対して送信する（ステップ９０４）。

【０１２６】次に、第４機器１１０１に備えられる機器間通信部４０５は、第３機器１００１より送信データＴ－Ｄａｔａ３を受信し、送信データＴ－Ｄａｔａ３より前記暗号化情報Ｅ３と前記ＣＳ５とを抽出する（ステップ９０５）。そして、機器間通信部４０５は、暗号化情報Ｅ３を暗号／復号部４０２へ、ＣＳ５をチェックサム判定部４０６へ送信する。

【０１２７】暗号／復号部４０２は、暗号化情報Ｅ３を受信すると、共通情報記憶部４０３より共通情報Ａを受信する。暗号／復号部４０２は暗号化情報Ｅ３を共通情報Ａを鍵として復号化を行い、復号済み暗号化対象データＤＲ２を取得し、チェックサム生成部４０４に送信する（ステップ９０６）。続いて、チェックサム生成部４０４は受信した復号済み暗号化対象データＤＲ２に対するＣＳ６を生成し、チェックサム判定部４０６へ送信する（ステップ９０７）。チェックサム判定部４０６は、受信したＣＳ５とＣＳ６との比較処理を行う（ステップ９０８）。

【０１２８】そして、比較処理の結果、チェックサム判定部４０６は、ＣＳ５＝ＣＳ６となった場合はチェックサム一致の制御コードを、ＣＳ５≠ＣＳ６の場合はチェックサム不一致の制御コードを応答データ生成部４０７に送信する。次に、応答データ生成部４０７は、チェックサム不一致の制御コードを受信した場合、応答データは生成しない（ステップ９０９）。

【０１２９】検索情報判別部１１０６においては、第３機器１００１の送信データＴ－Ｄａｔａ３の検索情報Ｃに当てはまるコンテンツＩＤに使用することのできるライセンスを有するか否かの判別を行い、当該ライセンスを有する場合には、ライセンス情報Ｃ２を付与した返信データＡ－Ｄａｔａ４の返信を行う（ステップ１５０２）。また、検索情報Ｃを満たさない場合には、本実施の形態２においても返信を行わない（ステップ１５０３）ものとして説明する。尚、返信データＡ－Ｄａｔａ４に検索情報Ｃに該当するものがないとするデータを記載することも可能である。

【０１３０】次に、検索情報判別部１１０６は、ライセンスＩＤ等のライセンス情報Ｃ２の生成を行い（ステップ１５０４）、次に、応答データ生成部４０７は制御コードを受信し、制御コードに応じた前記ライセンス情報Ｃ２を含む応答データＡＤを生成し、暗号／復号部４０２及びチェックサム生成部４０４に送信する（ステップ９１０）。

【０１３１】そして、暗号／復号部４０２は受信した前記応答データＡＤを保持している復号済み暗号化対象データＤＲ２から前記ランダム情報Ｒ２を抽出し、前記ランダム情報Ｒ２を鍵としてライセンス情報Ｃ２と応答データＡＤとの暗号化を行い、暗号化情報Ｅ４を生成し、機器間通信部４０５に送信する（ステップ９１１）。また、チェックサム生成部４０４は受信した応答データＡＤに対するＣＳ７を生成し、機器間通信部４０５に送信する（ステップ９１２）。機器間通信部４０５は、少なくとも暗号化情報Ｅ４と前記ＣＳ７とを含み、通信プロトコルに応じたメッセージヘッダ等を付した返信データＡ－Ｄａｔａ４を第３機器１００１に対して送信する（ステップ９１３）。

【０１３２】次に、第３機器１００１を構成する機器間通信部３０５は、前記第４機器１１０１よりＡ－Ｄａｔａ４を受信し、暗号化情報Ｅ４とＣＳ７とを抽出する（ステップ９１４）。次に、機器間通信部３０５は、暗号化情報Ｅ４を暗号／復号部３０２へ、ＣＳ７をチェックサム判定部３０６へ送信する。

【０１３３】暗号／復号部３０２は、機器間通信部３０５より暗号化情報Ｅ４を受信するとランダム情報生成部３０１よりランダム情報Ｒ２を受信する。暗号／復号部３０２は、受信した暗号化情報Ｅ４を保持していたランダム情報Ｒ２を鍵として復号化を行い、復号された暗号化情報（以下、復号済み応答データと呼ぶ）ＤＡ４を取得し、チェックサム生成部３０４及びチェックサム判定

部３０６に送信する（ステップ９１５）。続いて、チェックサム生成部３０４は受信した復号済み応答データＤＡ４に対するＣＳ８を生成し、チェックサム判定部３０６へ送信する（ステップ９１６）。チェックサム判定部３０６は受信したＣＳ７とＣＳ８の比較処理を行う（ステップ９１７）。

【０１３４】まず、比較処理の結果、ＣＳ７＝ＣＳ８となった場合は応答データＡＤを送信してきた第４機器１１０１が同一グループに属し、かつ検索対象のコンテンツに対応するライセンスを有すると判断し、チェックサム判定部３０６は、第４機器１１０１が有し検索対象となるライセンスをライセンスリスト１４０８に追加する（ステップ１５０５）。ＣＳ７≠ＣＳ８の場合は同一グループに属しないか、又は検索情報Ｃを満たさないと判断する（ステップ９１８）。尚、本実施の形態２においては、送信データＴ－Ｄａｔａ３及び返信データＡ－Ｄａｔａ４の暗号化対象部はそれぞれ暗号化対象データＥＤ及び応答データＡＤであるが、チェックサム５０５及びチェックサム６０５も含めて暗号化することができるのは言うまでもない。

【０１３５】以上のように、本実施の形態２に係る機器認証システムにおいては、第３機器１００１より送信される送信データＴ－Ｄａｔａ３は、ランダム情報５０３に加えて検索情報Ｃであるコンテンツ ＩＤ１２０１及びアクション ＩＤ１２０２を含む。そして、第４機器１１０１は、暗号化された暗号化対象データＥＤを共通情報Ａで復号化して、チェックサム５０５を比較判定することにより第３機器１００１が同一グループに属するか否かの判定を行い、同一グループに属する場合には、さらに、検索情報判別部１１０６において、前記コンテンツ ＩＤ１２０１及びアクション ＩＤ１２０２の検索対象となるコンテンツに適したライセンスを有しているか否かの判定を行い、判定の結果、検索情報Ｃを満たすライセンスを有する場合には、ライセンス ＩＤ１３０１、利用条件データ１３０２等を含む返信データＡ－Ｄａｔａ４を第３機器１００１へ返送する。

【０１３６】そして、第３機器１００１は、前記返信データＡ－Ｄａｔａ４を受信し、応答データＡＤをランダム情報５０３により復号化して、チェックサム６０５の一致判定を行うことにより、第４機器１１０１が同一グループに属し、かつ検索情報Ｃを満たすライセンスを有すると判断し、検索情報Ｃを満たすライセンスリスト１４０８を作成する。

【０１３７】このため、前記実施の形態１の作用効果に加えて、本実施の形態２における機器認証システムにおいては、第３機器１００１よりブロードキャストにより送信された送信データＴ－Ｄａｔａ３を受信した機器全てが返信データＡ－Ｄａｔａ４を返信するのではなく、同一グループに属し、かつ検索情報Ｃを満たすライセンスを有する機器のみが返信データＡ－Ｄａｔａ４を返信する。このため、第３機器１００１は、検索対象のライセンスを有する機器のライセンスリスト１４０８を作成して、このライセンスリスト１４０８に従うことによりライセンスの交換、購入等が可能な他の機器をより効率的に特定することができる。従って、本発明は、コンテンツ配信システムにおける端末機器間でのライセンス検索に適用することが可能である。

【０１３８】尚、上述した各実施の形態において、共通情報は、共通情報Ａを用いて説明したが、各機器が複数の共通情報も保持し、これら複数の共通情報を追加、削除等することにより、同一グループ範囲の設定についても柔軟かつ容易に実現できるようにすることも可能である。

【０１３９】

【発明の効果】以上の説明から明らかなように、本発明に係る機器認証システムにおいては、少なくとも第１及び第２機器から構成され、前記第１及び前記第２機器が同一のグループに属するか否かを判定する機器認証システムであって、前記第１機器は、共通情報を記憶する第１共通情報記憶手段と、鍵情報を含む送信データを生成する送信データ生成手段と、生成された送信データを前記共通情報で暗号化する第１暗号化手段と、前記第１暗号化手段で得られた暗号化送信データを前記第２機器に送信する第１送信手段と、前記第２機器から送られてきた暗号化返信データを前記鍵情報で復号化する第１復号化手段と、復号化された前記返信データが一定の規則を有するか否か判定し、一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断する認証手段とを備え、前記第２機器は、共通情報を記憶する第２共通情報記憶手段と、前記第１機器から送られてきた暗号化送信データを前記共通情報で復号化する第２復号化手段と、復号化された前記送信データが一定の規則を有するか否かを判定する判定手段と、前記送信データが一定の規則を有する場合に、前記第１及び第２機器は同一のグループに属すると判断し、その旨を示す返信データを生成する返信データ生成手段と、生成された返信データを前記復号化手段で復号された送信データに含まれていた鍵情報で暗号化する第２暗号化手段と、前記第２暗号化手段で得られた暗号化返信データを前記第１機器に送信する第２送信手段とを備える。

【０１４０】これによって、本発明に係る機器認証システムにおいては、各端末機器も対等の関係になる場合において同一グループに属する機器の特定を可能とし、また、端末機器が認証処理、コンテンツ送受信処理等の端末に負荷の大きい処理を行う前に、安全に同一グループに属する端末のグループリストを取得し、さらに、前記グループリストを利用することにより、送信データの送信先となる機器を決定して、コンテンツの取得が不可能な端末に対しては通信を行わずに、通信経路の効率的な利用等を可能とする。

【０１４１】また、本発明に係る機器認証システムにおいては、前記送信データ生成手段は、検索したい物を特定する情報である検索情報を前記送信データに含ませて前記送信データを生成し、前記第２機器は、さらに、復号化された前記送信データに含まれる検索情報が示す物を当該第２機器が保持するか否か判定する検索情報判定手段を備え、前記返信データ生成手段は、前記検索情報判定手段による判定結果を前記返信データに含ませて前記返信データを生成する。そして、前記送信データ生成手段は、デジタルコンテンツを特定するコンテンツＩＤを前記検索情報として前記送信データに含ませ、前記返信データ生成手段は、前記送信データに含まれているコンテンツＩＤが示すデジタルコンテンツの利用を可能にする権利情報であるライセンスを当該第２機器が保持する場合に、当該ライセンスを特定するライセンスＩＤを前記返信データに含ませる。

【０１４２】これらにより、本発明に係る機器認証システムにおいては、検索対象のライセンスを有する機器のライセンスリストを作成して、このライセンスリストに従うことによりライセンスの交換、購入等が可能な他の機器をより効率的に特定して、コンテンツ配信システムにおける端末機器間でのライセンス検索に適用することを可能とする。

【図面の簡単な説明】

【図１】実施の形態１に係る機器認証システムを説明する概略図である。

【図２】実施の形態１に係る複数の機器とグループとの関係を示す図である。

【図３】実施の形態１に係る第１機器の詳細な構成を示すブロック図である。

【図４】実施の形態１に係る第２機器の詳細な構成を示すブロック図である。

【図５】実施の形態１に係る送信データのデータ構成を示す図である。

【図６】実施の形態１に係る返信データのデータ構成を示す図である。

【図７】（ａ）は、実施の形態１におけるユーザインターフェイスの画面を示す図である。（ｂ）は、実施の形態１における別のユーザインターフェイスの画面を示す図である。

【図８】（ａ）は、実施の形態１における第１機器が作成するグループリストの情報項目を示す図である。（ｂ）は、実施の形態１における第１機器が作成する別のグループリストの情報項目を示す図である。

【図９】実施の形態１に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。

【図１０】実施の形態２に係る第３機器の詳細な構成を示すブロック図である。

【図１１】実施の形態２に係る第４機器の詳細な構成を示すブロック図である。

【図１２】実施の形態２に係る送信データのデータ構成を示す図である。

【図１３】実施の形態２に係る返信データのデータ構成を示す図である。

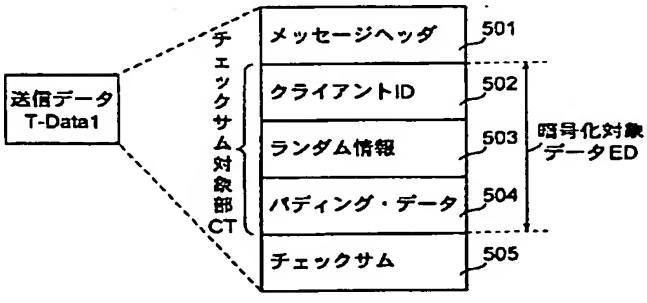
【図１４】実施の形態２に係る第３機器が検索情報を用いて第４機器及び第５機器にＬＴ検索を行う際の通信手順を示すシーケンス図である。

【図１５】実施の形態２に係る機器認証システムのグループ判定の処理手順を示すフローチャートである。

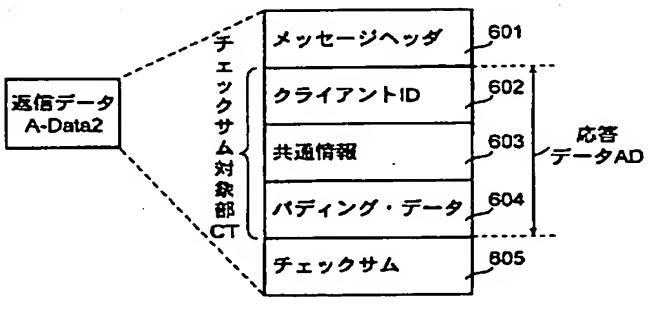
【符号の説明】

１０１　第１機器
１０２　第２機器
３０１　ランダム情報生成部
３０２，４０２　暗号／復号部
３０３，４０３　共通情報記憶部
３０４，４０４　チェックサム生成部
３０５，４０５　機器間通信部
３０６，４０６　チェックサム生成部
４０７　応答データ生成部
１００１　第３機器
１００１ａ，１１０１ａ　コンテンツ利用部
１００１ｂ，１１０１ｂ　端末管理部
１００５，１１０５　入力部
１００７　検索情報付与部
１１０１　第４機器
１１０６　検索情報判別部

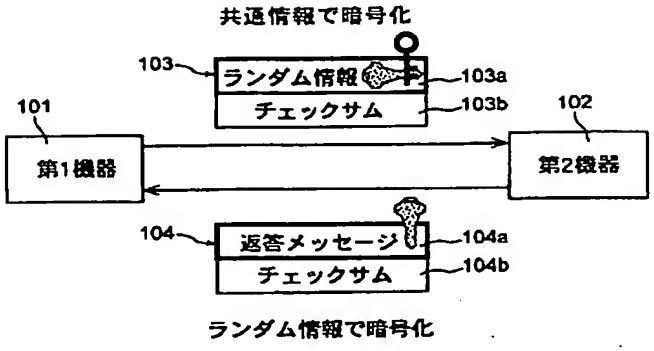
【図５】



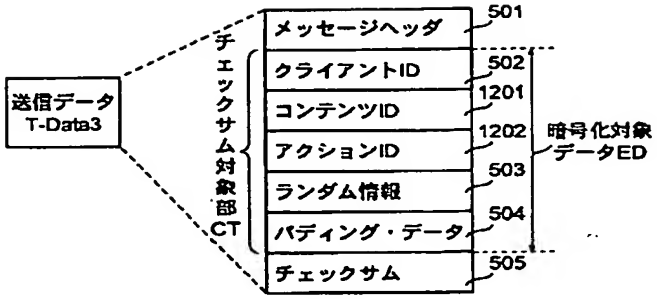
【図６】



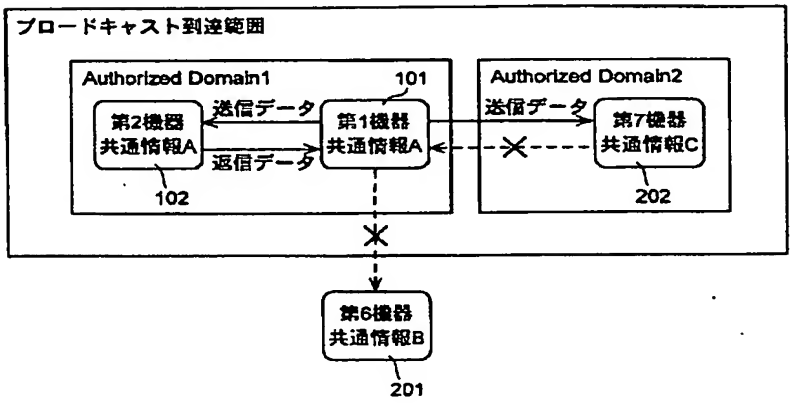
【図１】


共通情報で暗号化
103
ランダム情報
103a
チェックサム
103b
101
102
第1機器
第2機器
104
返答メッセージ
104a
チェックサム
104b
ランダム情報で暗号化

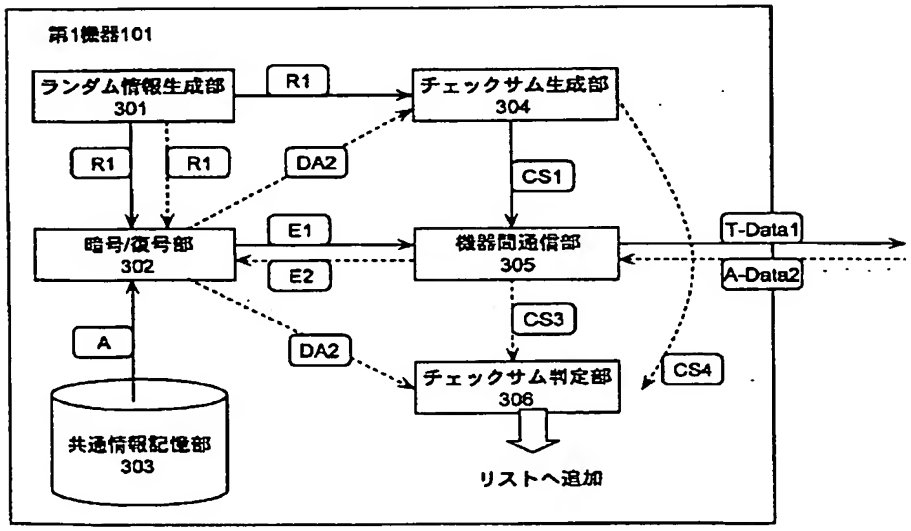
【図１２】


送信データ
T-Data3
チェックサム対象部CT
メッセージヘッダ
501
クライアントID
502
コンテンツID
1201
アクションID
1202
ランダム情報
503
パディング・データ
504
チェックサム
505
暗号化対象データED

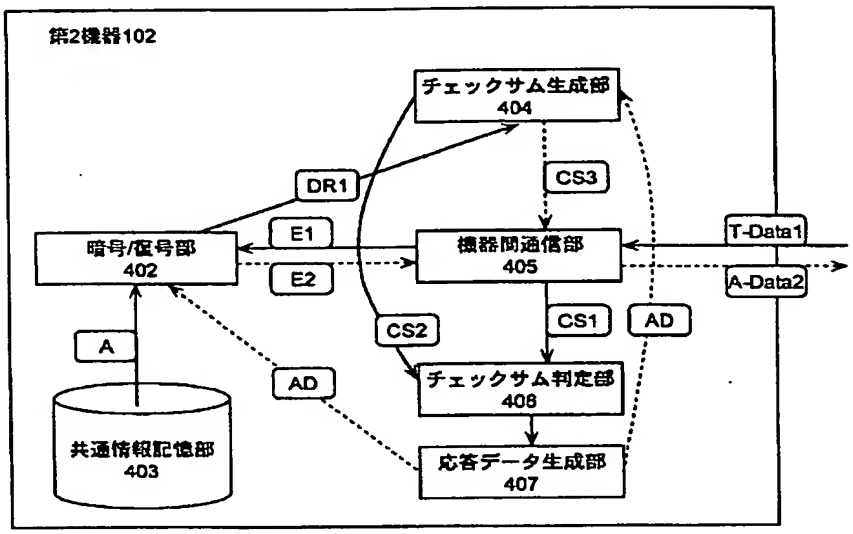
【図２】


ブロードキャスト到達範囲
Authorized Domain1
101
第2機器
共通情報A
送信データ
返信データ
第1機器
共通情報A
102
Authorized Domain2
送信データ
第7機器
共通情報C
202
第6機器
共通情報B
201

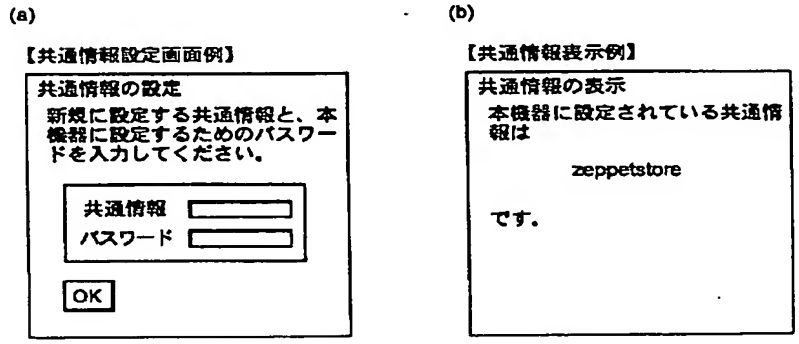
【図３】


第1機器101
ランダム情報生成部
301
R1
チェックサム生成部
304
R1
R1
DA2
CS1
暗号/復号部
302
E1
E2
機器間通信部
305
T-Data1
A-Data2
CS3
A
DA2
CS4
チェックサム判定部
306
共通情報記憶部
303
リストへ追加

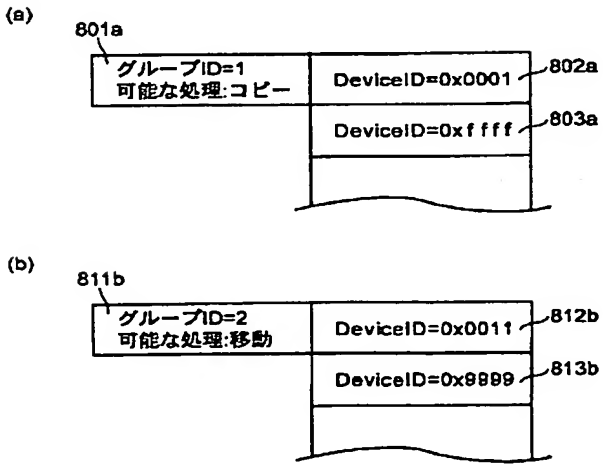
【図４】


第2機器102
チェックサム生成部
404
CS3
DR1
E1
暗号/復号部
402
E2
機器間通信部
405
T-Data1
A-Data2
CS2
CS1
AD
A
AD
チェックサム判定部
406
共通情報記憶部
403
応答データ生成部
407

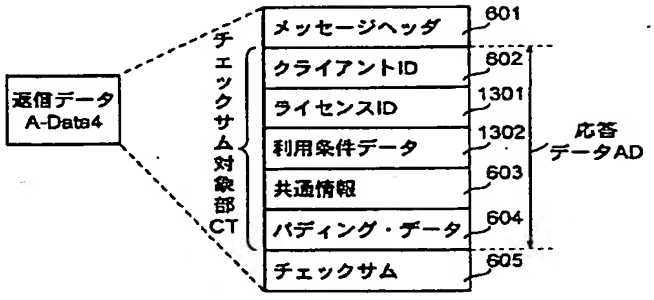
【図７】


(a)
【共通情報設定画面例】
共通情報の設定
新規に設定する共通情報と、本機器に設定するためのパスワードを入力してください。
共通情報
パスワード
OK
(b)
【共通情報表示例】
共通情報の表示
本機器に設定されている共通情報は
zeppetstore
です。

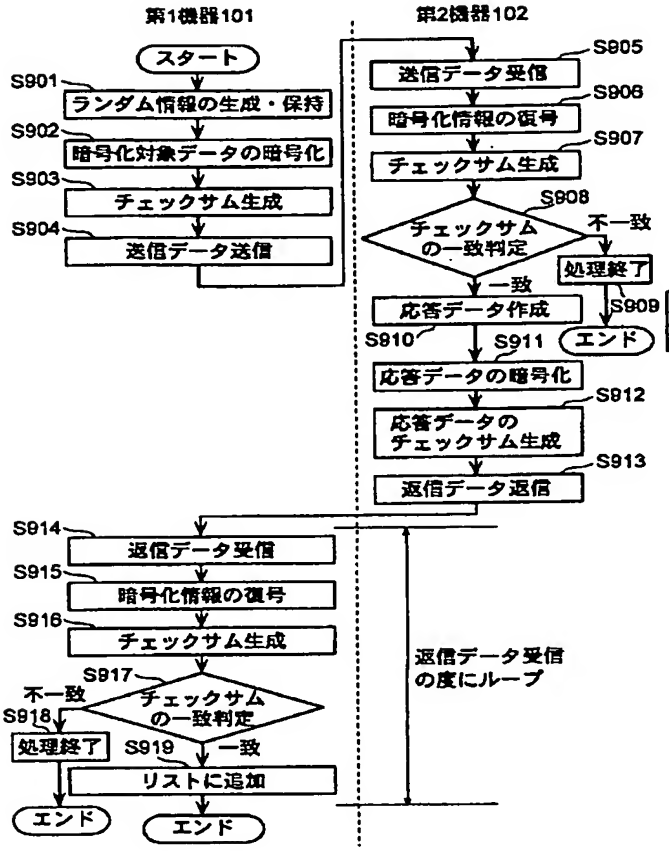
【図８】


(a)
801a
グループID=1
可能な処理:コピー
DeviceID=0x0001
802a
DeviceID=0xffff
803a
(b)
811b
グループID=2
可能な処理:移動
DeviceID=0x0011
812b
DeviceID=0x9999
813b

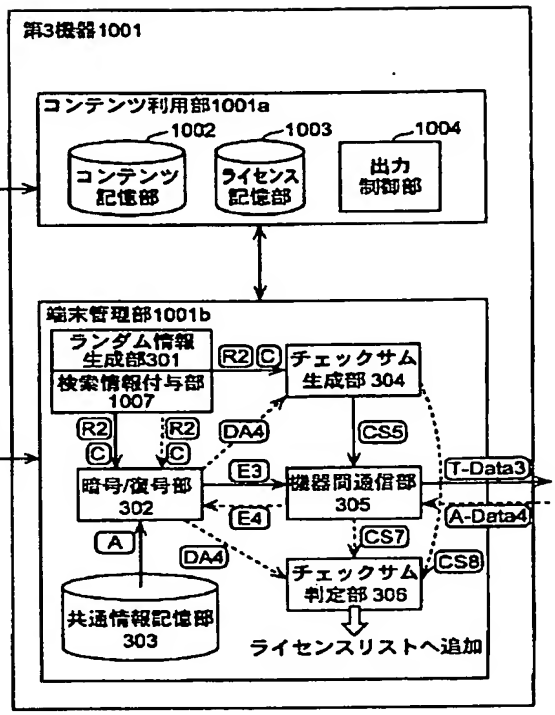
【図１３】


返信データ
A-Data4
チェックサム対象部CT
メッセージヘッダ
601
クライアントID
602
ライセンスID
1301
利用条件データ
1302
共通情報
603
パディング・データ
604
チェックサム
605
応答データAD

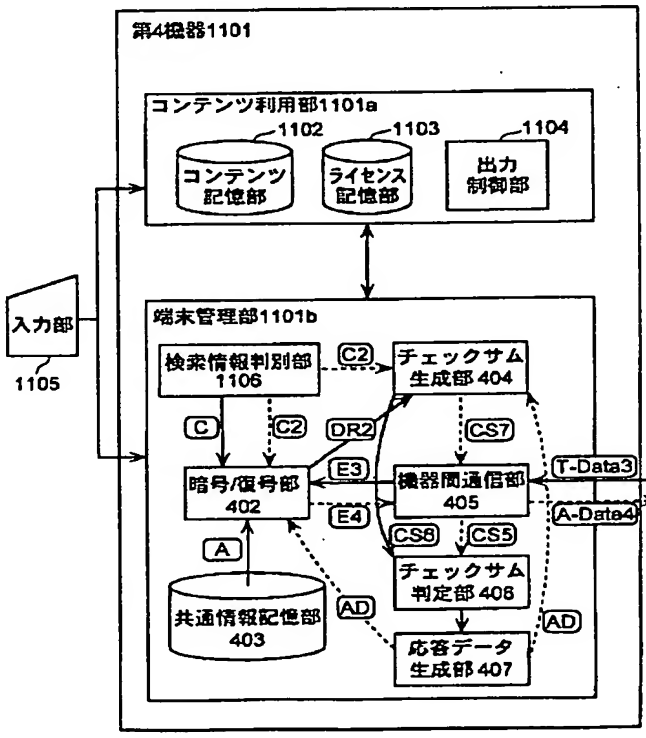
【図９】



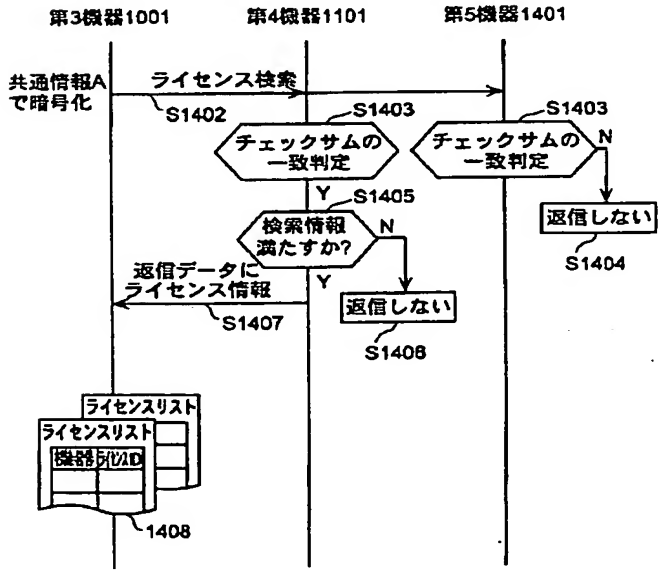
【図１０】



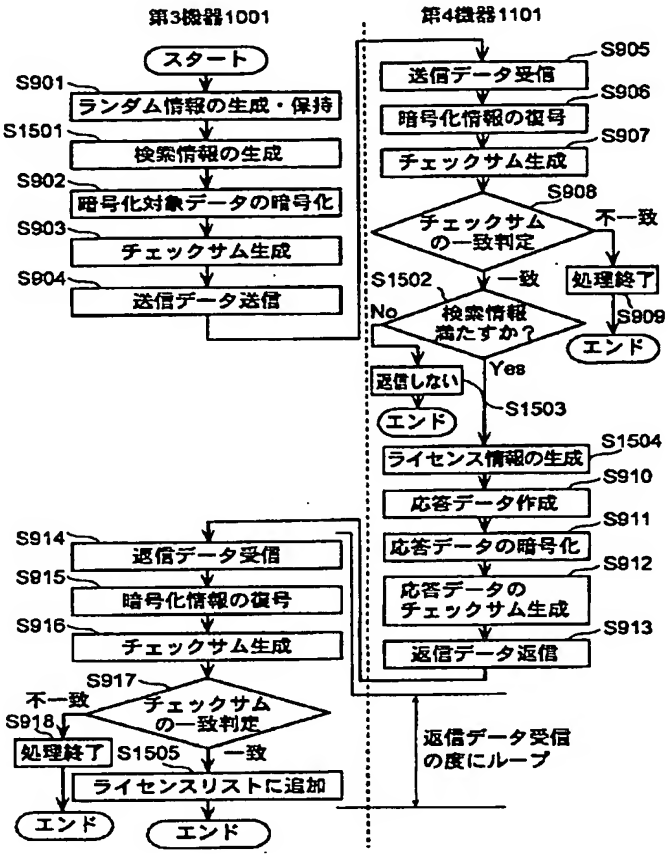
【図１１】



【図１４】



【図１５】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード（参考）
		H04L 9/00	601E

(72)発明者　中原　徹
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Fターム(参考)　5B085 AA08 AE06 AE23 BG01 BG02 BG07
5J104 AA07 AA16 EA04 EA16 EA18 GA05 KA02 KA04 KA06 NA02 PA07